

07.04.00

## 日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

REC'D 26 MAY 2000

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 4月12日

EKV

出 願 番 号

Application Number:

平成11年特許願第103992号

出 願 人

Applicant(s):

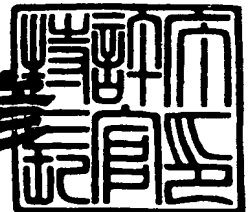
ソニー株式会社

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 5月12日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3034975

【書類名】 特許願

【整理番号】 9900015406

【提出日】 平成11年 4月12日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 石橋 義人

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項 1】 他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、

前記価値情報を復号するのに必要な鍵、前記価値情報の使用条件、および前記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶手段と、

前記記憶手段により記憶されている前記利用情報に含まれる前記使用条件が所定の条件で、かつ、前記利用情報に含まれる前記移動状態情報が、前記価値情報の移動が行われていないことを示しているとき、前記価値情報、および前記利用情報に含まれる前記鍵を含む所定の移動情報を前記他の情報処理装置に供給する供給手段と、

前記供給手段により、前記価値情報、および前記移動情報が前記他の情報処理装置に供給されたとき、前記移動状態情報の内容を、前記価値情報の移動が行われていることを示すものに変更する第 1 の変更手段と、

前記記憶手段により記憶されている前記利用情報に含まれる前記移動状態情報が、前記価値情報の移動が行われていることを示しており、前記情報処理装置への前記価値情報の移動を解除するとき、前記他の情報処理装置に所定の制御信号を送信する送信手段と、

前記他の情報処理装置から、前記送信手段により送信された前記制御信号に対する応答信号を受信したとき、前記移動状態情報の内容を、前記価値情報の移動が行われていないことを示すものに変更する第 2 の変更手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記記憶手段は、所定のメモリ領域に分割されている複数のブロックにより構成され、前記利用情報を、前記所定のメモリ領域に記憶し、

前記記憶手段を構成する前記ブロックに記憶されている複数の前記利用情報の全体にハッシュ関数を適用し、ハッシュ値を算出する算出手段と、

ハッシュ値を記憶するハッシュ値記憶手段と、

前記算出手段により算出された前記ハッシュ値と、前記ハッシュ値記憶手段に記憶されている所定のハッシュ値を比較し、比較結果に基づいて、前記記憶手段が改竄されたか否かを判定する判定手段と、

前記判定手段による判定結果に基づいて、前記供給手段による供給を制御する制御手段と

をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、

前記価値情報を復号するのに必要な鍵、前記価値情報の使用条件、および前記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記利用情報に含まれる前記使用条件が所定の条件で、かつ、前記利用情報に含まれる前記移動状態情報が、前記価値情報の移動が行われていないことを示しているとき、前記価値情報、および前記利用情報に含まれる前記鍵を含む所定の移動情報を前記他の情報処理装置に供給する供給ステップと、

前記供給ステップで、前記価値情報、および前記移動情報が前記他の情報処理装置に供給されたとき、前記移動状態情報の内容を、前記価値情報の移動が行われていることを示すものに変更する第 1 の変更ステップと、

前記記憶ステップで記憶されている前記利用情報に含まれる前記移動状態情報が、前記価値情報の移動が行われていることを示しており、前記情報処理装置への前記価値情報の移動を解除するとき、前記他の情報処理装置に所定の制御信号を送信する送信ステップと、

前記他の情報処理装置から、前記送信ステップで送信された前記制御信号に対する応答信号を受信したとき、前記移動状態情報の内容を、前記価値情報の移動が行われていないことを示すものに変更する第 2 の変更ステップと

を含むことを特徴とする情報処理方法。

【請求項 4】 他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、

前記価値情報を復号するのに必要な鍵、前記価値情報の使用条件、および前記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記利用情報に含まれる前記使用条件が所定の条件で、かつ、前記利用情報に含まれる前記移動状態情報が、前記価値情報の移動が行われていないことを示しているとき、前記価値情報、および前記利用情報に含まれる前記鍵を含む所定の移動情報を前記他の情報処理装置に供給する供給ステップと、

前記供給ステップで、前記価値情報、および前記移動情報が前記他の情報処理装置に供給されたとき、前記移動状態情報の内容を、前記価値情報の移動が行われていることを示すものに変更する第1の変更ステップと、

前記記憶ステップで記憶されている前記利用情報に含まれる前記移動状態情報が、前記価値情報の移動が行われていることを示しており、前記他の情報処理装置への前記価値情報の移動を解除するとき、前記他の情報処理装置に所定の制御信号を送信する送信ステップと、

前記他の情報処理装置から、前記送信ステップで送信された前記制御信号に対する応答信号を受信したとき、前記移動状態情報の内容を、前記価値情報の移動が行われていないことを示すものに変更する第2の変更ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項5】 他の情報処理装置に接続され、暗号化された前記価値情報を復号し、利用する情報処理装置において、

前記他の情報処理装置から供給される前記価値情報、および前記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信手段と、

前記受信手段により受信された前記移動情報を記憶する記憶手段と、

前記他の情報処理装置から、所定の制御信号を受信したとき、前記記憶手段に記憶されている前記移動情報を削除する削除手段と、

前記削除手段により、前記移動情報が削除されたとき、所定の応答信号を送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 6】 前記記憶手段は、所定のメモリ領域に分割されている複数のブロックにより構成され、前記移動情報を、前記所定のメモリ領域に記憶するし、

前記記憶手段の前記ブロックごとに記憶されている複数の前記移動情報の全体にハッシュ関数を適用し、ハッシュ値を算出する算出手段と、

ハッシュ値を記憶するハッシュ値記憶手段と、

前記算出手段により算出された前記ハッシュ値と、前記ハッシュ値記憶手段に記憶されている所定のハッシュ値を比較し、比較結果に基づいて、前記記憶手段が改竄されたか否かを判定する判定手段と、

前記判定手段による判定結果に基づいて、前記受信手段による受信を制御する制御手段と

をさらに備えることを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】 他の情報処理装置に接続され、暗号化された前記価値情報を復号し、利用する情報処理装置の情報処理方法において、

前記他の情報処理装置から供給される前記価値情報、および前記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、

前記受信ステップで受信された前記移動情報を記憶する記憶ステップと、

前記他の情報処理装置から、所定の制御信号を受信したとき、前記記憶ステップで記憶された前記移動情報を削除する削除ステップと、

前記削除ステップで、前記移動情報が削除されたとき、所定の応答信号を送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 8】 他の情報処理装置に接続され、暗号化された前記価値情報を復号し、利用する情報処理装置に、

前記他の情報処理装置から供給される前記価値情報、および前記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、

前記受信ステップで受信された前記移動情報を記憶する記憶ステップと、

前記他の情報処理装置から、所定の制御信号を受信したとき、前記記憶ステッ

ブで記憶された前記移動情報を削除する削除ステップと、

前記削除ステップで、前記移動情報が削除されたとき、所定の応答信号を送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並び提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

【0002】

【従来の技術】

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

【0003】

また、コンテンツを利用することができる情報処理装置が複数存在する場合、ユーザは、提供されてコンテンツを移動させ、コンテンツが移動された情報処理装置において、コンテンツを利用することもできる。

【0004】

【発明が解決しようとする課題】

しかしながら、この場合、コンテンツは移動元の情報処理装置が保持されず、ユーザが、移動元の情報処理装置において、そのコンテンツを利用できない課題があった。

【0005】

本発明はこのような状況に鑑みてなされたものであり、コンテンツが移動元の情報処理装置にも保持され、他の情報処理装置にコンテンツを移動させることができるようにするものである。

【0006】

## 【課題を解決するための手段】

請求項 1 に記載の情報処理装置は、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶手段と、記憶手段により記憶されている利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給手段と、供給手段により、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第 1 の変更手段と、記憶手段により記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信手段と、他の情報処理装置から、送信手段により送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第 2 の変更手段とを備えることを特徴とする。

## 【0007】

請求項 3 に記載の情報処理方法は、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、記憶ステップで記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給ステップと、供給ステップで、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第 1 の変更ステップと、記憶ステップで記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信ステップと、他の情報処理装置から、送信ステップ



で送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第2の変更ステップとを含むことを特徴とする。

## 【0008】

請求項4に記載の提供媒体は、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、記憶ステップで記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給ステップと、供給ステップで、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第1の変更ステップと、記憶ステップで記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信ステップと、他の情報処理装置から、送信ステップで送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第2の変更ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

## 【0009】

請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体においては、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報が記憶され、記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報が他の情報処理装置に供給され、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容が、価値情報の移動が行われて

いることを示すものに変更され、記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号が送信され、他の情報処理装置から、制御信号に対する応答信号が受信されたとき、移動状態情報の内容が、価値情報の移動が行われていないことを示すものに変更される。

#### 【0010】

請求項5に記載の情報処理装置は、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信手段と、受信手段により受信された移動情報を記憶する記憶手段と、他の情報処理装置から、所定の制御信号を受信したとき、記憶手段に記憶されている移動情報を削除する削除手段と、削除手段により、移動情報が削除されたとき、所定の応答信号を送信する送信手段とを備えることを特徴とする。

#### 【0011】

請求項7に記載の情報処理方法は、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、受信ステップで受信された移動情報を記憶する記憶ステップと、他の情報処理装置から、所定の制御信号を受信したとき、記憶ステップで記憶された移動情報を削除する削除ステップと、削除ステップで、移動情報が削除されたとき、所定の応答信号を送信する送信ステップとを含むことを特徴とする。

#### 【0012】

請求項8に記載の提供媒体は、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、受信ステップで受信された移動情報を記憶する記憶ステップと、他の情報処理装置から、所定の制御信号を受信したとき、記憶ステップで記憶された移動情報を削除する削除ステップと、削除ステップで、移動情報が削除されたとき、所定の応答信号を送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

#### 【0013】

請求項 5 に記載の情報処理装置、請求項 7 に記載の情報処理方法、および請求項 8 に記載の提供媒体においては、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報が受信され、受信された価値情報が記憶され、他の情報処理装置から、所定の制御信号を受信したとき、記憶された移動情報が削除され、移動情報が削除されたとき、所定の応答信号が送信される。

【0014】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0015】

図 1 は、本発明を適用した EMD (Electronic Music Distribution: 電子音楽配信) システムを説明する図である。EMD システムは、各装置を管理する EMD サービスセンタ 1、コンテンツを提供するコンテンツプロバイダ 2（この例の場合、2 式のコンテンツプロバイダ 2-1, 2-2（以下、個々に区別する必要がない場合、単に、コンテンツプロバイダ 2 と記述する。他の装置についても同様である）が設けられている）、コンテンツに対応するサービスを提供するサービスプロバイダ 3（この例の場合、2 式のサービスプロバイダ 3-1, 3-2 が設けられている）、およびコンテンツが利用されるユーザネットワーク 5 から構成されている。

【0016】

EMD システムにおけるコンテンツ (Content) とは、情報そのものが価値を有するデジタルデータで、この例の場合、1 つのコンテンツは、1 曲分の音楽データに相当する。またコンテンツは、1 つのコンテンツを 1 つの単位（シングル）として、または複数のコンテンツを 1 つの単位（アルバム）としてユーザに提供される。ユーザは、コンテンツを購入し（実際は、コンテンツを利用する権利を購入

し)、コンテンツを利用する。

【0017】

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5、およびコンテンツプロバイダ2に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

【0018】

コンテンツプロバイダ2-1, 2-2は、図2に示すように、提供するコンテンツ(コンテンツ鍵Kcoで暗号化されている)、そのコンテンツを復号するために必要なコンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、およびコンテンツの利用内容などを示す取扱方針(以下、UCP(Usage Control Policy)と記述する)を保持し、それらを、コンテンツプロバイダセキュアコンテナ(後述)と称する形態で、サービスプロバイダ3に供給する。

【0019】

サービスプロバイダ3-1, 3-2は、コンテンツプロバイダ2から供給されるUCPに対応して、1つまたは複数の価格情報(以下、PT(Price Tag)と記述する)を作成し、それを保持する。サービスプロバイダ2は、作成したPTを、コンテンツプロバイダ2から供給されたコンテンツ(コンテンツ鍵Kcoで暗号化されている)、コンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

【0020】

ユーザホームネットワーク5は、供給されたUCPおよびPTに基づいて、図2に示すように、使用許諾条件情報(以下、UCS(Usage Control Status)と称する)を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵Kdの供給を受けるタイミングで、対応するUCPおよびPTな

どとともにEMDサービスセンタ1に送信する。なお、ユーザホームネットワーク5は、UCPおよびPTをEMDサービスセンタ1に送信しないようにすることもできる。

#### 【0021】

この例の場合、ユーザホームネットワーク5は、HDD52に接続され、SAM(Secure Application Module)62を有するレシーバ51、およびHDD202に接続され、SAM212を有するレシーバ201から構成されている。レシーバ51とレシーバ201は、IEEE1394等で接続されている。

#### 【0022】

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信したり、利益分配の情報を供給する。

#### 【0023】

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)に送信する。

#### 【0024】

鍵サーバ14は、配送用鍵Kdを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

#### 【0025】

ユーザホームネットワーク5の機器(例えば、レシーバ51またはレシーバ201)およびコンテンツプロバイダ2に供給される、EMDサービスセンタ1からの配送用鍵Kdについて、図4乃至図7を参照して説明する。

#### 【0026】

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホーム

ネットワーク 5 を構成するレシーバ 51 がコンテンツの利用を開始する、1998 年 1 月における、EMD サービスセンタ 1 が有する配送用鍵 K d、コンテンツプロバイダ 2 が有する配送用鍵 K d、およびレシーバ 51 が有する配送用鍵 K d を示す図である。

## 【0027】

図 4 の例において、配送用鍵 K d は、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ” の値を有するバージョン 1 である配送用鍵 K d は、1998 年 1 月 1 日から 1998 年 1 月 31 日まで使用可能（すなわち、1998 年 1 月 1 日から 1998 年 1 月 31 日の期間にサービスプロバイダ 3 を介してユーザホームネットワーク 5 に配布されるコンテンツを暗号化するコンテンツ鍵 K c o は、バージョン 1 である配送用鍵 K d で暗号化されている）であり、所定のビット数の乱数である” b b b b b b b b ” の値を有するバージョン 2 である配送用鍵 K d は、1998 年 2 月 1 日から 1998 年 2 月 28 日まで使用可能（すなわち、その期間にサービスプロバイダ 3 を介してユーザホームネットワーク 5 に配布されるコンテンツを暗号化するコンテンツ鍵 K c o は、バージョン 2 である配送用鍵 K d で暗号化されている）である。同様に、バージョン 3 である配送用鍵 K d は、1998 年 3 月中に使用可能であり、バージョン 4 である配送用鍵 K d は、1998 年 4 月中に使用可能であり、バージョン 5 である配送用鍵 K d は、1998 年 5 月中に使用可能であり、バージョン 6 である配送用鍵 K d は、1998 年 6 月中に使用可能である。

## 【0028】

コンテンツプロバイダ 2 がコンテンツの提供を開始するに先立ち、EMD サービスセンタ 1 は、コンテンツプロバイダ 2 に、1998 年 1 月から 1998 年 6 月まで利用可能な、バージョン 1 乃至バージョン 6 の 6 つの配送用鍵 K d を送信し、コンテンツプロバイダ 2 は、6 つの配送用鍵 K d を受信し、記憶する。6 月分の配送用鍵 K d を記憶するのは、コンテンツプロバイダ 2 が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

## 【0029】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

## 【0030】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

## 【0031】

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

## 【0032】

1998年2月1日から1998年2月28日の期間には、バージョン2であ

る配送用鍵K d が、EMDサービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 5 1 で利用される。

【0033】

1998年3月1日における、EMDサービスセンタ 1 の配送用鍵K d のコンテンツプロバイダ 2、およびレシーバ 5 1 への送信を図 6 で説明する。EMDサービスセンタ 1 は、コンテンツプロバイダ 2 に、1998年3月から1998年8月まで利用可能な、バージョン 3 乃至バージョン 8 の 6 つの配送用鍵K d を送信し、コンテンツプロバイダ 2 は、6 つの配送用鍵K d を受信し、受信前に記憶していた配送用鍵K d に上書きし、新たな配送用鍵K d を記憶する。EMDサービスセンタ 1 は、レシーバ 5 1 に、1998年3月から1998年5月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵K d を送信し、レシーバ 5 1 は、3 つの配送用鍵K d を受信し、受信前に記憶していた配送用鍵K d に上書きし、新たな配送用鍵K d を記憶する。EMDサービスセンタ 1 は、バージョン 1 である配送用鍵K d およびバージョン 2 である配送用鍵K d をそのまま記憶する。

【0034】

1998年3月1日から1998年3月31日の期間には、バージョン 3 である配送用鍵K d が、EMDサービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 5 1 で利用される。

【0035】

1998年4月1日における、EMDサービスセンタ 1 の配送用鍵K d のコンテンツプロバイダ 2、およびレシーバ 5 1 への送信を図 7 で説明する。EMDサービスセンタ 1 は、コンテンツプロバイダ 2 に、1998年4月から1998年9月まで利用可能な、バージョン 4 乃至バージョン 9 の 6 つの配送用鍵K d を送信し、コンテンツプロバイダ 2 は、6 つの配送用鍵K d を受信し、受信前に記憶していた配送用鍵K d に上書きし、新たな配送用鍵K d を記憶する。EMDサービスセンタ 1 は、レシーバ 5 1 に、1998年4月から1998年6月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵K d を送信し、レシーバ 5 1 は、3 つの配送用鍵K d を受信し、受信前に記憶していた配送用鍵K d に上



書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K d、バージョン2である配送用鍵K d、およびバージョン3である配送用鍵K dをそのまま記憶する。

## 【0036】

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

## 【0037】

このように、あらかじめ先の月の配送用鍵K dを配布しておくことで、仮にユーザが1、2ヶ月まったくEMDサービスセンタ1にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ1にアクセスして鍵を受信することができる。

## 【0038】

ユーザホームネットワーク5の、EMDシステムに正式登録された機器、およびコンテンツプロバイダ2には、以上のように、3ヶ月分の配送用鍵K dが配布されるが、EMDシステムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク5の機器には、3ヶ月分の配送用鍵K dに代わり、図8に示すような、1ヶ月分の配送用鍵K dが配布される。この例においては、ユーザホームネットワーク5の機器をEMDシステムに正式登録するために、与信処理など、約1ヶ月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約1ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、1ヶ月間において利用可能な配送用鍵K dが配布される。

## 【0039】

図3に戻り、経歴データ管理部15は、ユーザ管理部18から出力される、課金情報、そのコンテンツに対応するPT、およびそのコンテンツに対応するUCPなどを記憶する。

## 【0040】

利益分配部16は、経歴データ管理部15から供給された各種情報に基づき、

EMDサービスセンタ1、コンテンツプロバイダ2-1, 2-2、およびサービスプロバイダ3-1, 3-2の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に出力する。利益配分部16はまた、算出した利益に応じてコンテンツプロバイダ2-1, 2-2およびサービスプロバイダ3-1, 3-2のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利用すればするほど、大きい値となるポイント）を算出し、ユーザ管理部18に出力する。なお、以下において、コンテンツプロバイダ2における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ3における利用ポイントをサービス利用ポイントと称する。

#### 【0041】

相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の機器と相互認証を実行する。

#### 【0042】

ユーザ管理部18は、ユーザホームネットワーク5の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図9に示すように、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に対応する所定の情報が含まれている。

#### 【0043】

「SAMのID」には、製造された、ユーザホームネットワーク5の機器のSAMのIDが記憶される。図9のシステム登録情報の「SAMのID」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDが設定されている。

#### 【0044】

「機器番号」には、SAMを有するユーザホームネットワーク5の機器に、予め設定された機器番号が設定されている。ユーザホームネットワーク5の機器が、ネットワーク4を介してサービスプロバイダ3と、およびEMDサービスセンタ1と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、UCPやPTの内容をユーザに出力（提示）したり、ユーザがUCPの利用内容を選択する

ことができる機能を有している（表示部および操作部を有している）場合、その機器（以下、主機器と称する）には、100番以上の機器番号が与えられる。機器が、そのような機能を有しない場合、その機器（以下、従機器と称する）には、99番以下の機器番号が与えられる。この例の場合、詳細は後述するが、レシーバ51およびレシーバ201の両者は、上述した機能を有しているので、それぞれには、100番以上の機器番号（100番）が与えられてる。そこで、図9のシステム登録情報の「機器番号」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDに対応する「機器番号」のそれぞれには、機器番号100番が設定されている。

#### 【0045】

「決済ID」には、EMDシステムに正式登録されたとき割り当てられる所定の決済IDが記憶される。この例の場合、レシーバ51およびレシーバ201は共に、正式登録され、決済IDが与えられているので、図9のシステム登録情報の、SAM62のIDおよびSAM212のIDに対応する「決済ID」のそれぞれには、その与えられた決済IDが記憶されている。

#### 【0046】

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ID、パスワードなどが設定される。

#### 【0047】

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別（以下、ここに区別する必要がない場合、これらの情報をまとめて、ユーザー一般情報と称する）は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうち、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対して、ユーザー一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユー

ザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに仮登録されるときに割り当てられ、設定される。

## 【0048】

図9のシステム登録情報には、レシーバ51のSAM62のIDに対応する「決済ユーザ情報」には、レシーバ51の決済ユーザである、ユーザFの、ユーザ一般情報、ID、およびパスワードが設定され、レシーバ201のSAM212のIDに対応する「決済ユーザ情報」には、レシーバ201の決済ユーザである、ユーザAの、ユーザ一般情報、ID、およびパスワードが設定されている。

## 【0049】

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよびパスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

## 【0050】

この例の場合、レシーバ51およびレシーバ201の両者には、従属ユーザが登録されていないので、図9のシステム登録情報のSAM62のIDに対応する「従属ユーザ情報」、およびSAM212のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

## 【0051】

「利用ポイント情報」には、利益分配部16から出力された利用ポイントが設定される。この例の場合、SAM62およびSAM212に対応する「利用ポイント情報」には、それぞれの利用ポイント情報が設定されている。図10は、レシーバ

51の利用ポイント情報の例を示している。図10の例では、レシーバ51のユーザF（決済ユーザ）に与えられている、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイントで、コンテンツプロバイダ2-2のコンテンツ利用ポイントが123ポイントで、サービスプロバイダ3-1のサービス利用ポイントが、345ポイントで、そして、サービスプロバイダ3-2のサービス利用ポイントが0ポイントであるとされている。

## 【0052】

なお、この例において、コンテンツプロバイダ2-1およびコンテンツプロバイダ2-2のそれぞれのコンテンツ利用ポイントの合計ポイント345（＝123＋222）と、サービスプロバイダ3-1およびサービスプロバイダ3-2のそれぞれのサービス利用ポイントの合計ポイント345（＝345＋0）が等しくなるようになされている。

## 【0053】

レシーバ201においては、現時点でコンテンツは利用されていないので、SAM212のIDに対応する「利用ポイント情報」には、何の情報の設定されていない。

## 【0054】

ユーザ管理部18は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Kdとともにユーザホームネットワーク5に送信する。

## 【0055】

図3に、再度戻り、課金請求部19は、経歴データ管理部15から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部20はまた、決算処理の結果をユーザ管理部18に通知する。

## 【0056】

監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、

PT、およびUCPの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、監査部 21 は、コンテンツプロバイダ 2 からの UCP を、サービスプロバイダ 3 からの PT を、そしてユーザホームネットワーク 5 からの、対応する UCP および PT を受け取る。

## 【0057】

図 11 は、コンテンツプロバイダ 2-1 の機能的構成を示すブロック図である。コンテンツサーバ 31 は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部 32 に供給する。ウォーターマーク付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部 33 に供給する。

## 【0058】

圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、ATRA C2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵（以下、この乱数をコンテンツ鍵  $K_c$  と称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

## 【0059】

乱数発生部 35 は、コンテンツ鍵  $K_c$  となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵  $K_c$  を EMD サービスセンタ 1 から供給された配送用鍵  $K_d$  を使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

## 【0060】

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

## 【0061】

まず、平文の64ビットは、上位32ビットの $H_0$ 、および下位32ビットの $L_0$ に分割される。鍵処理部から供給された48ビットの拡大鍵 $K_1$ 、および下位32ビットの $L_0$ を入力とし、下位32ビットの $L_0$ を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの $H_0$ と、F関数の出力が排他的論理和され、その結果は $L_1$ とされる。 $L_0$ は、 $H_1$ とされる。

## 【0062】

上位32ビットの $H_0$ および下位32ビットの $L_0$ を基に、以上の処理を16回繰り返し、得られた上位32ビットの $H_{16}$ および下位32ビットの $L_{16}$ が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

## 【0063】

ポリシー記憶部37は、コンテンツに対応して設定されるUCPを記憶し、セキュアコンテナ作成部38に出力する。図12は、コンテンツサーバ31に保持されているコンテンツAに対応して設定され、ポリシー記憶部37に記憶されているUCPA、Bを表している。UCPは、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「利用条件」、「利用内容」の各項目に対応する所定の情報が含まれる。「コンテンツのID」には、UCPが対応するコンテンツのIDが設定される。UCPA（図12（A））およびUCPB（図12（B））のそれぞれの「コンテンツのID」には、コンテンツAのIDが設定されている。

## 【0064】

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定される。UCPAおよびUCPBのそれぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが設定されている。「UCPのID」には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが、UCPBの「UCPのID」には、UCPBのIDが、それぞれ設定されている。「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCP

の有効期限」には、UCPAの有効期限が、UCPBの「UCPの有効期限」には、UCPBの有効期限が、それぞれ設定されている。

【0065】

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定され、「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる機器の条件が設定されている。

【0066】

UCPAの場合、「利用条件10」が設定され、「利用条件10」の「ユーザ条件10」には、利用ポイントが200ポイント以上であることが条件であることを示す情報（”200ポイント以上”）が設定されている。また「利用条件10」の「機器条件10」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、UCPAは、200ポイント以上のコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

【0067】

UCPBの場合、「利用条件20」が設定され、「利用条件20」の「ユーザ条件20」には、利用ポイントが200ポイントより少ないことが条件であることを示す情報（”200ポイントより少ない”）が設定されている。また「利用条件20」の「機器条件20」には、”条件なし”が設定されている。すなわち、UCPBは、200ポイントより少ないコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

【0068】

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

【0069】

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されて



いるか否か)を示す情報(“可”または“不可”)が設定される。コンテンツの管理移動が行われると、図13(A)に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図13(B)に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

## 【0070】

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図13(A)に示すように、他の機器にコンテンツを管理移動することができない(許可されない)。すなわち、管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。この点で、図14(A)に示すように、オリジナルのコンテンツから、複数の複製(第1世代)を作成することができる、第1世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図14(B)に示すように、1回だけの複製とも異なる。

## 【0071】

図12(A)に戻り、UCPAには、4つの「利用内容11」乃至「利用内容14」が設けられており、「利用内容11」において、その「ID11」には、「利用内容11」に割り当てられた所定のIDが設定されている。「形式11」には、コンテンツを買い取って再生する利用形式を示す情報(“買い取り再生”)が設定され、「パラメータ11」には、“買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報11」には、コンテンツの管理移動が許可されていることを示す情報(“可”)が設定されている。

## 【0072】

「利用内容12」において、その「ID12」には、「利用内容12」に割り当てられた所定のIDが設定されている。「形式12」には、第1世代の複製を行う利用形式を示す情報(“第1世代複製”)が設定されている。第1世代複製は、図14(A)に示したように、オリジナルのコンテンツから、複数の第1世代の

複製を作成することができる。ただし、第1世代の複製から第2世代の複製を作成することはできない（許可されない）。「パラメータ12」には、“第1世代複製”に対応する所定の情報が設定されている。「管理移動許可情報12」には、コンテンツの管理移動が許可されていないことを示す情報（“不可”）が設定されている。

## 【0073】

「利用内容13」において、その「ID13」には、「利用内容13」に割り当てられた所定のIDが設定されている。「形式13」には、所定の期間（時間）に限って再生する利用形式を示す情報（“期間制限再生”）が設定され、「パラメータ13」には、“期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報13」には、“不可”が設定されている。

## 【0074】

「利用内容14」において、その「ID14」には、「利用内容14」に割り当てられた所定のIDが設定されている。「形式14」には、5回の複製を行う利用形式（いわゆる、5回複製することができる回数券）を示す情報（“Pay Per Copy5”）が設定されている。なお、この場合も、図14の（B）に示すように、複製からの複製を作成することはできない（許可されない）。「パラメータ14」には、複製が5回可能であることを示す情報（“複製5回”）が設定されている。「管理移動許可情報14」には、“不可”が設定されている。

## 【0075】

図12（B）のUCPBには、2つの「利用内容21」、および「利用内容22」が設けられている。「利用内容21」において、その「ID21」には、「利用内容21」に割り当てられた所定のIDが設定されている。「形式21」には、4回の再生を行う利用形式を示す情報（“Pay Per Play4”）が設定され、「パラメータ21」には、再生が4回可能であることを示す情報（“再生4回”）が設定されている。「管理移動許可情報21」には、“不可”が設定されている。

## 【0076】

「利用内容22」において、その「ID22」には、「利用内容22」に割り当

てられた所定のIDが設定されている。「形式 2 2」には、“ Pay Per Copy 2 ” が設定され、「パラメータ 2 2」には、“ 複製 2 回 ” が設定されている。「管理移動許可情報 2 2」には、“ 不可 ” が設定されている。

#### 【0077】

ここで、UCPAおよびUCPBの内容を比較すると、200ポイント以上の利用ポイントを有するユーザは、4通りの利用内容11乃至利用内容14から利用内容を選択することができるのに対して、200ポイントより少ない利用ポイントを有するユーザは、2通りの利用内容21，22からしか利用内容を選択することができないものとされている。

#### 【0078】

ところで、図12は、UCPAおよびUCPBを模擬的に表しているが、例えば、UCPAの「利用条件10」およびUCPBの「利用条件20」には、実際は、図15（A）に示すサービスコード、および図15（B）に示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードがそれぞれ設定されている。

#### 【0079】

図16（A）は、UCPA（図12（A））の「利用条件10」の「ユーザ条件10」および「機器条件10」として設定されている各コードのコード値を表している。UCPAの「利用条件10」の「ユーザ条件10」は、“ 200ポイント以上 ” とされているので、“ 利用ポイントに関し条件有り ” を意味する80xxhのサービスコード（図15（A））が、このとき数値200を示す0000C8hのバリューコードが、そして“ ≥（以上） ” を意味する06hのコンディションコード（図15（B））が、ユーザ条件として設定されている。

#### 【0080】

UCPAの「機器条件10」は、“ 条件なし ” とされているので、“ 条件なし ” を意味する0000hのサービスコードが、このとき何ら意味を持たないFFFFFFhのバリューコードが、そして“ 無条件 ” を意味する00hのコンディションコードが、機器条件として設定されている。

#### 【0081】

図16 (B) は、UCPBの「利用条件20」の「ユーザ条件20」および「機器条件20」として設定されている各コードのコード値を表している。「ユーザ条件20」は、「200ポイントより少ない」とされているので、「利用ポイントに関し条件有り」を意味する80xxhのサービスコードが、数値200を示す0000C8hのバリューコードが、そして「<(より小さい)」を意味する03hのコンディションコードが、ユーザ条件として設定されている。

#### 【0082】

UCPBの「機器条件20」は、UCPAの「機器条件10」と同様に、「条件なし」とされ、同一のコード値が設定されているので、その説明は省略する。

#### 【0083】

図11に戻り、セキュアコンテナ作成部38は、例えば、図17に示すような、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、UCPA、B、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、およびUCPA、Bの全体）にハッシュ関数を適用して得られたハッシュ値が、公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ2-1の秘密鍵Kscp）で暗号化されたものである。

#### 【0084】

セキュアコンテナ作成部38はまた、コンテンツプロバイダセキュアコンテナに、図18に示すコンテンツプロバイダ2-1の証明書を付してサービスプロバイダ3に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2-1に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ2-1の名前、コンテンツプロバイダ2-1の公開鍵Kpcp、並びにその署名（認証局の秘密鍵Kscaで暗号化されている）から構成されている。

#### 【0085】

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信し

たいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0086】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0087】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【0088】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0089】

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である $p$ および $q$ を求め、さらに $p$ と $q$ の積である $n$ を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 $L$ を算出し、更に、3以上 $L$ 未満で、かつ、 $L$ と互いに素な数 $e$ を求める（すなわち、 $e$ と $L$ を共通に割り切れる数は、1のみである）。

## 【0090】

次に、 $L$ を法とする乗算に関する $e$ の乗法逆元 $d$ を求める。すなわち、 $d$ 、 $e$ 、および $L$ の間には、 $ed=1 \bmod L$ が成立し、 $d$ はユークリッドの互除法で算出できる。このとき、 $n$ と $e$ が公開鍵とされ、 $p, q$ , および $d$ が、秘密鍵とされる。

## 【0091】

暗号文 $C$ は、平文 $M$ から、式(1)の処理で算出される。

## 【0092】

$$C=M^e \bmod n \quad (1)$$

暗号文 $C$ は、式(2)の処理で平文 $M$ に、復号される。

## 【0093】

$$M=C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

## 【0094】

$$M=C^d=(M^e)^d=M^{(ed)}=M \bmod n \quad (3)$$

秘密鍵 $p$ と $q$ を知っているならば、公開鍵 $e$ から秘密鍵 $d$ は算出できるが、公開鍵 $n$ の素因数分解が計算量的に困難な程度に公開鍵 $n$ の桁数を大きくすれば、公開鍵 $n$ を知るだけでは、公開鍵 $e$ から秘密鍵 $d$ は計算できず、復号できない。以上のよう、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

## 【0095】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2=x^3+ax+b$ 上の、ある点を $B$ とする。楕円曲線上の点の加算を定義し、 $nB$ は、 $B$ を $n$ 回加算した結果を表す。同様に、減算も定義する。 $B$ と $nB$ から $n$ を算出することは、困難であることが証明されている。 $B$ と $nB$ を公開鍵とし、 $n$ を秘密鍵とする。乱数 $r$ を用いて、暗号文 $C1$ および $C2$ は、平文 $M$ から、公開鍵で式(4)および式(5)の処理で算出される。

## 【0096】

$$C1=M+rnB \quad (4)$$

$$C2=rB \quad (5)$$

暗号文C1およびC2は、式(6)の処理で平文Mに、復号される。

【0097】

$$M=C1-nC2 \quad (6)$$

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0098】

図11に、再び戻り、コンテンツプロバイダ2-1の相互認証部39は、EMDサービスセンタ1から配送用鍵Kdの供給を受けるのに先立ち、EMDサービスセンタ1と相互認証する。また相互認証部39は、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密しなければならない情報が含まれていないので、この相互認証は必ずしも必要とされるわけではない。

【0099】

コンテンツプロバイダ2-2は、コンテンツプロバイダ2-1と基本的の同様の構成を有しているので、その図示および説明は省略する。

【0100】

次に、図19のブロック図を参照して、サービスプロバイダ3-1の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ(コンテンツ鍵Kcoで暗号化されている)、コンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

【0101】

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ2の証明書が

検証され、正当であるとき、コンテンツプロバイダ2の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

#### 【0102】

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部42は、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部44に供給する。図20は、図12(A)のUCPAに対応して作成された、2つのPTA-1(図20(A))およびPTA-2(図20(B))を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に対応する所定の情報が含まれる。

#### 【0103】

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」には、UCPに対応する項目の情報が、それぞれ設定される。すなわち、PTA-1およびPTA-2のそれぞれの「コンテンツのID」には、コンテンツAのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、そしてそれぞれの「UCPのID」には、UCPAのIDが設定されている。

#### 【0104】

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ2のIDが設定される。PTA-1およびPTA-2のそれぞれの「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定される。PTA-1の「PTのID」には、PTA-1のIDが、PTA-2の「PTのID」には、PTA-2のIDがそれぞれ設定されている。

「PTの有効期限」には、PTの有効期限を示す情報が設定される。PTA-1の「PTの有効期限」には、PTA-1の有効期限が、PTA-2の「PTの有効期限」には、PTA-2の有効期限が設定されている。

#### 【0105】

「価格条件」には、UCPの「利用条件」と同様に、「ユーザ条件」および「機



器条件」の各項目に対応する所定の情報が設定されている。「価格条件」の「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

#### 【0106】

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（”男性”）が設定され、その「機器条件10」には、”条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

#### 【0107】

PTA-1の「価格条件10」の「ユーザ条件10」および「機器条件10」も、実際は、図21（A）に示すように、各種コードのコード値が設定されている。「価格条件10」の「ユーザ条件10」には、”性別条件有り”を意味する01xxhのサービスコード（図15（A））が、このとき男性を意味する000000hのバリューコードが、そして”=”を意味する01hのコンディションコード（図15（B））が設定されている。「機器条件10」には、”条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

#### 【0108】

PTA-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ条件20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件20」には、”条件なし”が設定されている。すなわち、PTA-2は、女性のユーザのみが選択可能となる。

#### 【0109】

PTA-2の「価格条件20」の「ユーザ条件20」および「機器条件20」も、実際は、図21（B）に示すように、各コードのコード値が設定されている。「価格条件20」の「ユーザ条件20」には、”性別条件有り”を意味する01xxhのサービスコード（図15（A））が、この場合女性を示す000001

hのバリューコードが、そして”=”を意味する01hのコンディションコード（図15（B））が設定されている。その「機器条件20」には、”条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

#### 【0110】

図20に戻り、PTの「価格内容」には、コンテンツが、対応するUCPの「利用内容」の「形式」に設定されている利用形式で利用される場合の利用料金が示されている。すなわち、PTA-1の「価格内容11」に設定された”2000円”およびPTA-2の「価格内容21」に設定された”1000円”は、UCPA（図12（A））の「利用内容11」の「形式11」が”買い取り再生”とされているので、コンテンツAの買い取り価格（料金）を示している。

#### 【0111】

PTA-1の「価格内容12」の”600円”およびPTA-2の「価格内容22」の”300円”は、UCPAの「利用内容12」の「形式12」より、第1世代複製の利用形式でコンテンツAを利用する場合の料金を示している。PTA-1の「価格内容13」の”100円”およびPTA-2の「価格内容23」の”50円”は、UCPAの「利用内容13」の「形式13」より、期間制限再生の利用形式でコンテンツAを利用する場合の料金を示している。PTA-1の「価格内容14」の”300円”およびPTA-2の「価格内容24」の”150円”は、UCPAの「利用内容14」の「形式14」より、5回の複製を行う利用形式でコンテンツAを利用する場合の料金を示している。

#### 【0112】

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1の価格内容に示される価格が、PTA-2の価格内容に示される価格の2倍に設定されている。例えば、UCPAの「利用内容11」に対応するPTA-1の「価格内容11」が”2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は”1000円”とされている。同様に、PT

A-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格の2倍とされている。すなわち、コンテンツAは、女性のユーザがより低価格で利用できるコンテンツとされている。

#### 【0113】

図22は、図12(B)のUCPBに対応して作成された、2つのPTB-1およびPTB-2を表している。図22(A)のPTB-1には、コンテンツAのID、コンテンツプロバイダ2-1のID、UCPBのID、サービスプロバイダ3-1のID、PTB-1のID、PTB-1の有効期限、価格条件30、2通りの価格内容31、32などが含まれている。

#### 【0114】

PTB-1の「価格条件30」の「ユーザ条件30」には”条件なし”が設定され、「機器条件30」には、機器が従機器であることを条件とする情報(”従機器”)が設定されている。すなわち、PTB-1は、コンテンツAが従機器において利用される場合にのみ選択可能となる。

#### 【0115】

PTB-1の「価格条件30」の「ユーザ条件30」および「機器条件30」にも、実際は、図23(A)に示すように、各コードのコード値が設定されている。「ユーザ条件30」には、”条件なし”を意味する0000hのサービスコード(図15(A))が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード(図15(B))が設定されている。「機器条件30」は、”従機器”とされているので、”機器に関し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”<(小さい)”を意味する03hのコンディションコードが設定されている。この例の場合、従機器には、100番より小さい機器番号が設定されているので、このようなコード値が設定される。

#### 【0116】

PTB-1の「価格内容31」の”100円”は、UCPB(図12(B))の「

利用内容 2 1」の「形式 2 1」が” Pay Per Play 4 ”とされているので、4 回の再生を行う場合の料金を示し、「価格内容 3 2」の” 3 0 0 円”は、UCPB の「利用内容 2 2」の「形式 2 2」が” Pay Per Copy 2 ”とされているので、2 回の複製を行う場合の料金を示している。

## 【0 1 1 7】

UCPB に対応して作成された、もう一方の PTB-2 には、図 2 2 (B) に示すように、コンテンツ A の ID、コンテンツプロバイダ 2-1 の ID、UCPB の ID、サービスプロバイダ 3-1 の ID、PTB-2 の ID、PTB-2 の有効期限、価格条件 4 0、および 2 通りの価格内容 4 1, 4 2 などが含まれている。

## 【0 1 1 8】

PTB-2 の「価格条件 4 0」の「ユーザ条件 4 0」には” 条件なし”が設定され、その「機器条件 4 0」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、PTB-2 は、主機器においてコンテンツが利用される場合にのみ選択可能となる。

## 【0 1 1 9】

PTB-2 の「価格条件 4 0」の「ユーザ条件 4 0」および「機器条件 4 0」にも、実際は、図 2 3 (B) に示すように、各コードのコード値が設定されている。「価格条件 4 0」の「ユーザ条件 4 0」には、” 条件なし”を意味する 0 0 0 0 h のサービスコード（図 1 5 (A)）が、この場合何ら意味を持たない F F F F F F h のバリューコードが、そして” 無条件”を意味する 0 0 h のコンディションコード（1 5 (B)）が設定されている。「機器条件 4 0」には、” 機器に関し条件有り”を意味する 0 0 x x h のサービスコードが、このとき” 数値 1 0 0 ”を示す 0 0 0 0 6 4 h のバリューコードが、そして” => (以上)”を意味する 0 6 h のコンディションコードが設定されている。この例の場合、主機器には、1 0 0 番以上の機器番号が設定されているので、このようなコード値が設定される。

## 【0 1 2 0】

PTB-2 の「価格内容 4 1」および「価格内容 4 2」のそれぞれに示される価格は、UCPB の「利用内容 2 1」の「形式 2 1」および「利用内容 2 2」の「形

式 22」のそれぞれに示される利用形式でコンテンツ A を利用する場合の料金を示している。

#### 【0121】

ここで、PTB-1（従機器に適用される）の価格内容と PTB-2（主機器に適用される）の価格内容を比較すると、PTB-1 の価格内容は、PTB-2 の価格内容の 2 倍に設定されている。例えば、PTB-1 の「価格内容 31」が” 100 円”とされているのに対し、PTB-2 の「価格内容 41」は 50 円とされており、「価格内容 32」が” 300 円”とされているのに対して、「価格内容 42」は” 150 円”とされている。

#### 【0122】

図 19 に戻り、ポリシー記憶部 43 は、コンテンツプロバイダ 2 から供給された、コンテンツの UCP を記憶し、セキュアコンテナ作成部 44 に供給する。

#### 【0123】

セキュアコンテナ作成部 44 は、例えば、図 24 に示すような、コンテンツ A（コンテンツ鍵 Kc o A で暗号化されている）、コンテンツ鍵 Kc o A（配送用鍵 Kd で暗号化されている）、UCPA、B、コンテンツプロバイダ 2 の署名、PTA-1、A-2、B-1、B-2、およびサービスプロバイダ 3 の署名からなるサービスプロバイダセキュアコンテナを作成する。

#### 【0124】

セキュアコンテナ作成部 44 はまた、作成したサービスプロバイダセキュアコンテナを、図 25 に示すような、証明書のバージョン番号、認証局がサービスプロバイダ 3-1 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3-1 の名前、サービスプロバイダ 3-1 の公開鍵 Kps p、並びに署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク 5 に供給する。

#### 【0125】

図 19 に、再び戻り、相互認証部 45 は、コンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロ

バイダ 2 と相互認証する。相互認証部 4 5 また、ユーザホームネットワーク 5 へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク 5 と相互認証するが、このサービスプロバイダ 3 とユーザホームネットワーク 5 との相互認証は、例えば、ネットワーク 4 が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ 3 は、コンテンツプロバイダ 2 およびユーザホームネットワーク 5 と相互認証を行わなくてもよい。

## 【0126】

サービスプロバイダ 3-2 の構成は、サービスプロバイダ 3-1 の構成と基本的に同様であるので、その図示および説明は省略する。

## 【0127】

次に、図 26 のブロック図を参照して、ユーザホームネットワーク 5 を構成するレシーバ 5 1 の構成例を説明する。レシーバ 5 1 は、通信部 6 1、SAM 6 2、外部記憶部 6 3、伸張部 6 4、通信部 6 5、インタフェース 6 6、表示制御部 6 7、および入力制御部 6 8 より構成されている。通信部 6 1 は、ネットワーク 4 を介してサービスプロバイダ 3、または EMD サービスセンタ 1 と通信し、所定の情報を受信し、または送信する。

## 【0128】

SAM 6 2 は、相互認証モジュール 7 1、課金処理モジュール 7 2、記憶モジュール 7 3、復号/暗号化モジュール 7 4、およびデータ検査モジュール 7 5 からなるが、シングルチップの暗号処理専用 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパ性）を有している。

## 【0129】

SAM 6 2 の相互認証モジュール 7 1 は、記憶モジュール 7 3 に記憶されている、図 2 7 に示す SAM 6 2 の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵  $K_{temp}$ （セッション

鍵) を復号/暗号化モジュール 74 に供給する。SAM の証明書には、コンテンツプロバイダ 2-1 の証明書およびサービスプロバイダ 3-1 の証明書に含まれている情報に対応する情報が含まれているので、その説明は省略する。

#### 【0130】

課金処理モジュール 72 は、選択された UCP の利用内容に基づいて、UCS および課金情報を作成する。図 28 は、図 12 (A) に示した UCPA の利用内容 11 と、図 20 (A) に示した PTA-1 の価格内容 11 に基づいて作成された UCSA を表している。UCS には、図 28 に示されるように、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「サービスプロバイダの ID」、「PT の ID」、「PT の有効期限」、「UCS の ID」、「SAM の ID」、「ユーザの ID」、「利用内容」、および「利用履歴」の各項目に対応する所定の情報が設定される。

#### 【0131】

UCS の、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「サービスプロバイダの ID」、「PT の ID」、および「PT の有効期限」の各項目には、PT の、それらに対応する項目の情報が設定される。すなわち、図 28 の UCSA の、「コンテンツの ID」には、コンテンツ A の ID が、「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2-1 の ID が、「UCP の ID」には、UCPA の ID が、「UCP の有効期限」には、UCPA の有効期限が、「サービスプロバイダの ID」には、サービスプロバイダ 3-1 の ID が、「PT の ID」には、PTA-1 の ID が、そして「PT の有効期限」には、PTA-1 の有効期限が、それぞれ設定されている。

#### 【0132】

「UCS の ID」には、UCS に割り当てられた所定の ID が設定され、UCSA の「UCS の ID」には、UCSA の ID が設定されている。「SAM の ID」には、機器の SAM の ID が設定され、UCSA の「SAM の ID」には、レシーバ 51 の SAM 62 の ID が設定されている。「ユーザの ID」には、コンテンツを利用するユーザの ID が設定され、UCSA の「ユーザの ID」には、ユーザ F の ID が設定されている。

#### 【0133】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容11」の「ID11」に設定されている情報（利用内容11のID）が、「形式」には、「利用内容11」の「形式11」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容11」の「パラメータ11」に設定されている情報（”買い取り再生”に対応する情報）が設定されている。

#### 【0134】

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDが、管理移動先の機器のIDとしても設定される。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われず（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容11」の「管理移動許可情報11」に”可”が設定されており、また、このとき、コンテンツAは管理移動されていないので、SAM62のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

#### 【0135】

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が設定される。UCSAの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ51において、コンテンツAが以前に利用されていた場合、そのときの利用形式も記憶される。

#### 【0136】

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上



述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

## 【0137】

作成されたUCSは、レシーバ51の復号／暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図29に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

## 【0138】

図29の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図28に示したUCSAと、コンテンツAを復号するためのコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1、RP-2には、他のコンテンツ鍵Kco1、Kco2（それぞれ保存用鍵Ksaveで暗号化されている）およびUCS1、2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4（図示せず）乃至RP-N、およびブロックBP-2（図示せず）乃至BP-Mには、この場合、コンテンツ鍵KcoおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域RPに記憶されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

## 【0139】

図30は、図28に示したUCSAと同時に作成された課金情報Aを表している

。課金情報は、図30に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」の各項目に対応する所定の情報が設定される。

#### 【0140】

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定される。すなわち、図30の課金情報Aの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが、「PTのID」には、PTA-1のIDが、「PTの有効期限」には、PTA-1の有効期限が、「UCSのID」には、UCSAのIDが、「SAMのID」には、SAM62のIDが、「ユーザのID」には、ユーザFのIDが、そして「利用内容」には、UCSAの「利用内容11」の内容が、それぞれ設定されている。

#### 【0141】

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報が設定される。課金情報Aの「課金履歴」には、レシーバ51において計上された課金の合計額が設定されている。

#### 【0142】

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているが、それらを課金情報に設定しないようにすることもできる。また、上述した課金情報においては、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプ

ロバイダを特定することができる場合、それを設けないようにすることもできる。

#### 【0143】

図26に戻り、記憶モジュール73には、図31に示すように、SAM62の公開鍵K<sub>pu</sub>、SAM62の秘密鍵K<sub>su</sub>、EMDサービスセンタ1の公開鍵K<sub>psc</sub>、認証局の公開鍵K<sub>pca</sub>、保存用鍵K<sub>save</sub>、3月分の配送用鍵K<sub>d</sub>などの各種鍵、SAM62の証明書（図27）、課金情報（例えば、図30の課金情報A）、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

#### 【0144】

図32は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定情報などが含まれている。

#### 【0145】

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」には、EMDサービスセンタ1のユーザ管理部18により管理されるシステム登録情報（図9）の、それらに対応する項目の情報が、それぞれ設定される。すなわち、基準情報51には、SAM62のID、SAM62の機器番号（100番）、ユーザFの決済ID、ユーザFの決済ユーザ情報（ユーザFの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザFのID、およびユーザFのパスワード）、および図33に示す利用ポイント情報（図10に示したものと同様の情報）が設定されている。

#### 【0146】

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる課金の上限額が設定される。基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（「正式登録時の上限額」）が設

定されている。なお、正式登録されている状態における課金の上限額は、仮登録されている状態における課金の上限額よりも、大きな額である。

#### 【0147】

次に、記憶モジュール73に記憶される、図31に示したM個の検査値HP-1乃至HP-Mについて説明する。検査値HP-1は、外部記憶部63の利用情報記憶部63AのブロックBP-1に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータのハッシュ値である。

#### 【0148】

図26に戻り、SAM62の復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、必要に応じ（例えば、相互認証時に）、所定の桁数の乱数を発生し、一時鍵Ktempを生成し、暗号化ユニット93に出力する。

#### 【0149】

暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、記憶モジュール73に保持されている保存用鍵Ksaveで暗号化する。暗号化されたコンテンツ鍵Kcoは、外部記憶部63に供給される。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部64に送信するとき、コンテンツ鍵Kcoを乱数発生ユニット92で生成した一時鍵Ktempで暗号化する。

#### 【0150】

データ検査モジュール75は、記憶モジュール73に記憶されている検査値HPと、外部記憶部63の利用情報記憶部63Aの、対応するブロックBPのデータのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査する。データ検査モジュール75はまた、コンテンツの購入、利用、および管理移動等が行われる際に、検査値HPを算出し、記憶モジュール73に記憶（更新）させる。

## 【0151】

伸張部 64 は、相互認証モジュール 101、復号モジュール 102、復号モジュール 103、伸張モジュール 104、およびウォーターマーク付加モジュール 105 から構成される。相互認証モジュール 101 は、SAM 62 と相互認証し、一時鍵 *Ktemp* を復号モジュール 102 に出力する。復号モジュール 102 は、一時鍵 *Ktemp* で暗号化されたコンテンツ鍵 *Kco* を一時鍵 *Ktemp* で復号し、復号モジュール 103 に出力する。復号モジュール 103 は、HDD 52 に記録されたコンテンツをコンテンツ鍵 *Kco* で復号し、伸張モジュール 104 に出力する。伸張モジュール 104 は、復号されたコンテンツを、更に ATRAC2 等の方式で伸張し、ウォーターマーク付加モジュール 105 に出力する。ウォーターマーク付加モジュール 105 は、コンテンツにレシーバ 51 を特定するための情報（例えば、SAM 62 の ID）のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

## 【0152】

通信部 65 は、ユーザホームネットワーク 5 のレシーバ 201 との通信処理を行う。インターフェース 66 は、SAM 62 および伸張部 64 からの信号を所定の形式に変更し、HDD 52 に出力し、また、HDD 52 からの信号を所定の形式に変更し、SAM 62 および伸張部 64 に出力する。

## 【0153】

表示制御部 67 は、表示部（図示せず）への出力を制御する。入力制御部 68 は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

## 【0154】

HDD 52 は、サービスプロバイダ 3 から供給されたコンテンツの他、図 34 に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象 SAM 情報部より構成されている。

## 【0155】

対象 SAM 情報部には、この登録リストを保有する機器の SAMID、この例の場合、レシーバ 51 の SAM 62 の ID が（「対象 SAMID」の欄に）記憶されている。対象 SA

M情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51は、レシーバ201に接続されているので、自分自身を含む値2が（「接続されている機器数」の欄に）記憶されている。

## 【0156】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件として、それぞれの項目に所定の情報が記憶されている。

## 【0157】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDが記憶されている。「ユーザID」には、対応する機器のユーザのIDが記憶される。この例の場合、ユーザFのIDおよびユーザAのIDが記憶されている。

## 【0158】

「購入処理」には、対応する機器が、コンテンツを購入（正確には、コンテンツを利用する権利を購入）するための処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツを購入するための処理を行うことができるので、“可”が記憶されている。

## 【0159】

「課金処理」には、対応する機器が、EMDサービスセンタ1との間で、課金を決済する処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51は、ユーザFが決済ユーザとして登録されており、レシーバ201は、ユーザAが決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、“可”が記憶されている。

## 【0160】

「課金機器」には、対応する機器において計上された課金に対する課金を決済する処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51（SAM62）およびレシーバ201（SAM212）は、自分自身の課金に対する決済を行うことができるので、SAM62のIDおよびSAM212のIDが記憶されている。

## 【0161】

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツの供給をサービスプロバイダ3から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。なお、ここで意味するコンテンツの供給は、管理移動によるものは含まれない。

## 【0162】

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、決済が成功しなかった場合、その機器に対応する「状態フラグ」には、”制限あり”が設定される。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

## 【0163】

この例の場合、レシーバ51およびレシーバ201に対しては、何ら制限が課せられていないものとし、「状態フラグ」には”なし”が設定されている。

## 【0164】

「登録条件署名」には、登録条件として、それぞれ、「SAMID」、「ユーザID

」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。この例の場合、レシーバ51およびレシーバ201の登録条件に対する署名が記憶されている。

#### 【0165】

「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が設定されている。

#### 【0166】

図35は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その詳細な説明は適宜省略する。

#### 【0167】

外部記憶部213は、図36に示すように、P個のブロックBM-1乃至BM-Pに分割され（例えば、1メガバイト毎に分割され）、各ブロックBMが、Q個の移動情報用メモリ領域RM-1乃至RM-Qに分割されている移動情報記憶部213Aを有しており、例えば、コンテンツが管理移動されたとき、SAM212から送信される、そのコンテンツに対応したコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）、コンテンツのID、および管理移動元の機器のSAMのID（以下、個々に区別する必要がない場合、これらをまとめて、移動情報と称する）を記憶する。

#### 【0168】

図36の移動情報記憶部213AのブロックBM-1の移動情報用メモリ領域RM-2には、コンテンツA（コンテンツ鍵Kcoで暗号化されている）に対応するコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）、コンテンツAのID、およびSAM62のIDが記憶されている。すなわち、レシーバ51から、コンテンツAが管理移動されている状態の移動情報記憶部213Aを表している。

#### 【0169】

なお、ブロックBM-1の移動情報用メモリ領域RM-2（図示せず）乃至RM



ーQ、およびブロックBM-2（図示せず）乃至BM-Pには、移動情報が記憶されておらず、空いている（移動情報を記憶することができる）ことを示す初期情報が記憶されている。

## 【0170】

SAM212の記憶モジュール223には、図37に示すように、SAM212の公開鍵K<sub>pu</sub>、SAM212の秘密鍵K<sub>su</sub>、EMDサービスセンタ1の公開鍵K<sub>pes</sub>c、認証局の公開鍵K<sub>pc</sub>a、保存用鍵K<sub>save</sub>、3月分の配送用鍵K<sub>d</sub>、予め認証局から配布されているSAM212の証明書、基準情報201、およびQ個の検査値HM-1乃至HM-Qが記憶されている。

## 【0171】

P個の検索値HM-1乃至HM-Qは、外部記憶部213の移動情報記憶部213Aの、各ブロックBM-1乃至BM-Qの記憶されているデータにハッシュ関数が適用されて算出されたハッシュ値である。

## 【0172】

HDD202は、HDD52と同様の機能を有するので、その説明は省略するが、HDD202には、図34のレシーバ51の登録リストのリスト部に示された、レシーバ51の登録条件およびレシーバ201の登録条件が設定されたリスト部を有するレシーバ201の登録リスト（図示せず）が記憶されている。

## 【0173】

なお、この例の場合、簡単のために、レシーバ51の外部記憶部63には、利用情報記憶部63Aのみが設けられ、またレシーバ201の外部記憶部213には、移動情報記憶部213Aのみが設けられているようにしたが、実際は、レシーバ51の外部記憶部63には、利用情報記憶部63Aの他、移動情報記憶部（図示せず）も設けられている。同様に、レシーバ201の外部記憶部213にも、移動情報記憶部213Aの他、利用情報記憶部（図示せず）が設けられている。

## 【0174】

次に、EMDシステムの処理について、図38のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ2-1に保持されているコンテンツA

が、サービスプロバイダ 3-1 を介して、ユーザホームネットワーク 5 のレシーバ 5 1 に供給され、利用される場合を例として説明する。

#### 【0 1 7 5】

ステップ S 1 1 において、配送用鍵 K d が、EMD サービスセンタ 1 からコンテンツプロバイダ 2-1 に供給される処理が行われる。この処理の詳細は、図 3 9 のフローチャートに示されている。すなわち、ステップ S 3 1 において、EMD サービスセンタ 1 の相互認証部 1 7 (図 3) は、コンテンツプロバイダ 2-1 の相互認証部 3 9 (図 1 1) と相互認証し、コンテンツプロバイダ 2-1 が、正当なプロバイダであることが確認した後、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 は、鍵サーバ 1 4 から供給された配送用鍵 K d をコンテンツプロバイダ 2-1 に送信する。なお、相互認証処理の詳細は、図 4 0 乃至図 4 2 を参照して後述する。

#### 【0 1 7 6】

次に、ステップ S 3 2 において、コンテンツプロバイダ 2-1 の暗号化部 3 6 は、EMD サービスセンタ 1 から送信された配送用鍵 K d を受信し、ステップ S 3 3 において、配送用鍵 K d を記憶する。

#### 【0 1 7 7】

このように、コンテンツプロバイダ 2-1 の暗号化部 3 6 が、配送用鍵 K d を記憶したとき、処理は終了し、図 3 8 のステップ S 1 2 に進む。ここで、ステップ S 1 2 以降の処理の説明の前に、図 3 9 のステップ S 3 1 における相互認証処理 (なりすましが無いことを確認する処理) について、1 つの共通鍵を用いる場合 (図 4 0)、2 つの共通鍵を用いる場合 (図 4 1)、および公開鍵暗号を用いる場合 (図 4 2) を例として説明する。

#### 【0 1 7 8】

図 4 0 は、1 つの共通鍵で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 3 9 と EMD サービスセンタ 1 の相互認証部 1 7 との相互認証の動作を説明するフローチャートである。ステップ S 4 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、6 4 ビットの乱数 R 1 を生成する (乱数生成部 3 5 が生成するようにしてもよい)。ステップ S 4 2 において、コンテン

プロバイダ 2 の相互認証部 39 は、DES を用いて乱数  $R_1$  を、予め記憶している共通鍵  $K_c$  で暗号化する（暗号化部 36 で暗号化するようにしてもよい）。ステップ S 43 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数  $R_1$  を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0179】

ステップ S 44 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数  $R_1$  を予め記憶している共通鍵  $K_c$  で復号する。ステップ S 45 において、EMD サービスセンタ 1 の相互認証部 17 は、32 ビットの乱数  $R_2$  を生成する。ステップ S 46 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した 64 ビットの乱数  $R_1$  の下位 32 ビットを乱数  $R_2$  で入れ替え、接続  $R_{1H} \parallel R_2$  を生成する。なお、ここで  $R_{iH}$  は、 $R_i$  の上位ビットを表し、 $A \parallel B$  は、 $A$  と  $B$  の接続（ $n$  ビットの  $A$  の下位に、 $m$  ビットの  $B$  を結合して、 $(n+m)$  ビットとしたもの）を表す。ステップ S 47 において、EMD サービスセンタ 1 の相互認証部 17 は、DES を用いて  $R_{1H} \parallel R_2$  を共通鍵  $K_c$  で暗号化する。ステップ S 48 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化した  $R_{1H} \parallel R_2$  をコンテンツプロバイダ 2 に送信する。

【0180】

ステップ S 49 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した  $R_{1H} \parallel R_2$  を共通鍵  $K_c$  で復号する。ステップ S 50 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号した  $R_{1H} \parallel R_2$  の上位 32 ビット  $R_{1H}$  を調べ、ステップ S 41 で生成した、乱数  $R_1$  の上位 32 ビット  $R_{1H}$  と一致すれば、EMD サービスセンタ 1 が正当なセンタであることを認証する。生成した乱数  $R_{1H}$  と、受信した  $R_{1H}$  が一致しないとき、処理は終了される。両者が一致するとき、ステップ S 51 において、コンテンツプロバイダ 2 の相互認証部 39 は、32 ビットの乱数  $R_3$  を生成する。ステップ S 52 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信し、復号した 32 ビットの乱数  $R_2$  を上位に設定し、生成した乱数  $R_3$  をその下位に設定し、接続  $R_2 \parallel R_3$  とする。ステップ S 53 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて接続  $R_2 \parallel R_3$  を共通鍵  $K_c$  で暗号化する。ステップ S 54 において、コンテン

コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された接続  $R2 \parallel R3$  を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0181】

ステップ S55 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した接続  $R2 \parallel R3$  を共通鍵  $Kc$  で復号する。ステップ S56 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した接続  $R2 \parallel R3$  の上位 32 ビットを調べ、乱数  $R2$  と一致すれば、コンテンツプロバイダ 2 を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0182】

図 41 は、2 つの共通鍵  $Kc1$ 、 $Kc2$  で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S61 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数  $R1$  を生成する。ステップ S62 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて乱数  $R1$  を予め記憶している共通鍵  $Kc1$  で暗号化する。ステップ S63 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数  $R1$  を EMD サービスセンタ 1 に送信する。

【0183】

ステップ S64 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数  $R1$  を予め記憶している共通鍵  $Kc1$  で復号する。ステップ S65 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数  $R1$  を予め記憶している共通鍵  $Kc2$  で暗号化する。ステップ S66 において、EMD サービスセンタ 1 の相互認証部 17 は、64 ビットの乱数  $R2$  を生成する。ステップ S67 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数  $R2$  を共通鍵  $Kc2$  で暗号化する。ステップ S68 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された乱数  $R1$  および乱数  $R2$  をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

【0184】

ステップ S69 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信

した乱数  $R_1$  および乱数  $R_2$  を予め記憶している共通鍵  $K_{c2}$  で復号する。ステップ  $S70$  において、コンテンツプロバイダ 2 の相互認証部 39 は、復号した乱数  $R_1$  を調べ、ステップ  $S61$  で生成した乱数  $R_1$  (暗号化する前の乱数  $R_1$ ) と一致すれば、EMD サービスセンタ 1 を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップ  $S71$  において、コンテンツプロバイダ 2 の相互認証部 39 は、復号して得た乱数  $R_2$  を共通鍵  $K_{c1}$  で暗号化する。ステップ  $S72$  において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数  $R_2$  を EMD サービスセンタ 1 に送信する。

## 【0185】

ステップ  $S73$  において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数  $R_2$  を共通鍵  $K_{c1}$  で復号する。ステップ  $S74$  において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数  $R_2$  が、ステップ  $S66$  で生成した乱数  $R_2$  (暗号化する前の乱数  $R_2$ ) と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

## 【0186】

図 42 は、公開鍵暗号である、160 ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ  $S81$  において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数  $R_1$  を生成する。ステップ  $S82$  において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵  $K_{pcp}$  を含む証明書 (認証局から予め取得しておいたもの) と、乱数  $R_1$  を EMD サービスセンタ 1 の相互認証部 17 に送信する。

## 【0187】

ステップ  $S83$  において、EMD サービスセンタ 1 の相互認証部 17 は、受信した証明書の署名 (認証局の秘密鍵  $K_{sca}$  で暗号化されている) を、予め取得しておいた認証局の公開鍵  $K_{pca}$  で復号し、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  および

コンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵  $K_{pcp}$  およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵  $K_{pcp}$  が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

## 【0188】

適正な認証結果が得られたとき、ステップ S 8 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、64 ビットの乱数  $R_2$  を生成する。ステップ S 8 5 において、EMD サービスセンタ 1 の相互認証部 1 7 は、乱数  $R_1$  および乱数  $R_2$  の接続  $R_1 \parallel R_2$  を生成する。ステップ S 8 6 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続  $R_1 \parallel R_2$  を自分自身の秘密鍵  $K_{sec}$  で暗号化する。ステップ S 8 7 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続  $R_1 \parallel R_2$  を、ステップ S 8 3 で取得したコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  で暗号化する。ステップ S 8 8 において、EMD サービスセンタ 1 の相互認証部 1 7 は、秘密鍵  $K_{sec}$  で暗号化された接続  $R_1 \parallel R_2$ 、公開鍵  $K_{pcp}$  で暗号化された接続  $R_1 \parallel R_2$ 、および自分自身の公開鍵  $K_{pec}$  を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ 2 の相互認証部 3 9 に送信する。

## 【0189】

ステップ S 8 9 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵  $K_{pca}$  で復号し、正しければ証明書から公開鍵  $K_{pec}$  を取り出す。この場合の処理は、ステップ S 8 3 における場合と同様であるので、その説明は省略する。ステップ S 9 0 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、EMD サービスセンタ 1 の秘密鍵  $K_{sec}$  で暗号化されている接続  $R_1 \parallel R_2$  を、ステップ S 8 9 で取得し

た公開鍵  $K_{pesc}$  で復号する。ステップ S91において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵  $K_{pcp}$  で暗号化されている接続  $R1 \parallel R2$  を、自分自身の秘密鍵  $K_{scp}$  で復号する。ステップ S92において、コンテンツプロバイダ2の相互認証部39は、ステップ S90で復号された接続  $R1 \parallel R2$  と、ステップ S91で復号された接続  $R1 \parallel R2$  を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

## 【0190】

適正な認証結果が得られたとき、ステップ S93において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数  $R3$  を生成する。ステップ S94において、コンテンツプロバイダ2の相互認証部39は、ステップ S90で取得した乱数  $R2$  および生成した乱数  $R3$  の接続  $R2 \parallel R3$  を生成する。ステップ S95において、コンテンツプロバイダ2の相互認証部39は、接続  $R2 \parallel R3$  を、ステップ S89で取得した公開鍵  $K_{pesc}$  で暗号化する。ステップ S96において、コンテンツプロバイダ2の相互認証部39は、暗号化した接続  $R2 \parallel R3$  をEMDサービスセンタ1の相互認証部17に送信する。

## 【0191】

ステップ S97において、EMDサービスセンタ1の相互認証部17は、暗号化された接続  $R2 \parallel R3$  を自分自身の秘密鍵  $K_{sesc}$  で復号する。ステップ S98において、EMDサービスセンタ1の相互認証部17は、復号した乱数  $R2$  が、ステップ S84で生成した乱数  $R2$  (暗号化する前の乱数  $R2$ ) と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

## 【0192】

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵  $K_{temp}$  として利用される。

## 【0193】

次に、図38のステップ S12の処理について説明する。ステップ S12にお

いては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2-1からサービスプロバイダ3-1に供給される処理が行われる。その処理の詳細は、図43のフローチャートに示されている。すなわち、ステップS201において、コンテンツプロバイダ2-1のウォーターマーク付加部32（図11）は、コンテンツサーバ31からコンテンツAを読み出し、コンテンツプロバイダ2-1を示す所定のウォーターマーク（電子透かし）を挿入し、圧縮部33に供給する。

## 【0194】

ステップS202において、コンテンツプロバイダ2-1の圧縮部33は、ウォーターマークが挿入されたコンテンツAをATRAC2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS203において、乱数発生部35は、コンテンツ鍵Kc○Aとなる乱数を発生させ、暗号化部34に供給する。

## 【0195】

ステップS204において、コンテンツプロバイダ2-1の暗号化部34は、DESなどの所定の方式で、乱数発生部35で発生された乱数（コンテンツ鍵Kc○A）を使用して、ウォーターマークが挿入されて圧縮されたコンテンツAを暗号化する。次に、ステップS205において、暗号化部36は、DESなどの所定の方式で、EMDサービスセンタ1から供給された配送用鍵Kdでコンテンツ鍵Kc○Aを暗号化する。

## 【0196】

ステップS206において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵Kc○Aで暗号化されている）、コンテンツ鍵Kc○A（配送用鍵Kdで暗号化されている）、およびポリシー記憶部37に記憶されている、コンテンツAに対応するUCPA、B（図12）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Kscpで暗号化する。これにより、図17に示した署名が作成される。

## 【0197】

ステップS207において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵Kc○Aで暗号化されている）、コ



ンテンツ鍵K c o A（配送用鍵K dで暗号化されている）、UCPA, B（図12）、およびステップS206で生成した署名を含んだ、図17に示したコンテンツプロバイダセキュアコンテナを作成する。

【0198】

ステップS208において、コンテンツプロバイダ2-1の相互認証部39は、サービスプロバイダ3-1の相互認証部45（図19）と相互認証する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、その説明は省略する。ステップS209において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、認証局から予め発行された証明書（図18）を、ステップS207で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ3-1に送信する。

【0199】

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ3-1に供給されたとき、処理は終了し、図38のステップS13に進む。

【0200】

ステップS13において、サービスプロバイダセキュアコンテナが、サービスプロバイダ3-1からユーザホームネットワーク5（レシーバ51）に供給される。この処理の詳細は、図44のフローチャートに示されている。すなわち、ステップS221において、サービスプロバイダ3-1の値付け部42（図19）は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図18）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2-1の公開鍵K p c pを取り出す。証明書の署名の確認は、図42のステップS83における処理と同様であるので、その説明は省略する。

【0201】

ステップS222において、サービスプロバイダ3-1の値付け部42は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2-1の公開鍵K p c pで復号し、得られたハッシュ値が、コンテンツA（コンテンツ鍵K c o Aで暗号化されている）、コン

テンツ鍵K c o A（配送用鍵K dで暗号化されている）、およびUCPA，Bの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップS 2 2 3に進む。

#### 【0202】

ステップS 2 2 3において、サービスプロバイダ3-1の値付け部42は、コンテンツプロバイダセキュアコンテナから、コンテンツA（コンテンツ鍵K c o Aで暗号化されている）、コンテンツ鍵K c o A（配送用鍵K dで暗号化されている）、および署名を取り出し、コンテンツサーバ41に供給する。コンテンツサーバ41は、それらを記憶する。値付け部42はまたUCPA，Bも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部44に供給する。

#### 【0203】

ステップS 2 2 4において、サービスプロバイダ3-1の値付け部42は、取り出したUCPA，Bに基づいて、PTA-1，A-2（図20）、およびPTB-1，B-2（図22）を作成し、セキュアコンテナ作成部44に供給する。

#### 【0204】

ステップS 2 2 5において、サービスプロバイダ3-1のセキュアコンテナ作成部44は、コンテンツサーバ41から読み出したコンテンツA（コンテンツ鍵K c o Aで暗号化されている）およびコンテンツ鍵K c o A（配送用鍵K dで暗号化されている）と、値付け部42から供給された、UCPA，B、およびPTA-1，A-2，B-1，B-2、並びにその署名から、図24に示したサービスプロバイダセキュアコンテナを作成する。

#### 【0205】

ステップS 2 2 6において、サービスプロバイダ3-1の相互認証部45は、レシーバ51の相互認証モジュール71（図26）と相互認証する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、その説明を

省略する。

【0206】

ステップS227において、サービスプロバイダ3-1のセキュアコンテナ作成部44は、ステップS225で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ3-1の証明書(図25)を付して、ユーザホームネットワーク5のレシーバ51に送信する。

【0207】

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ3-1からレシーバ51に送信されたとき、処理は終了し、図38のステップS14に進む。

【0208】

ステップS14において、サービスプロバイダ3-1から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク5のレシーバ51により受信される。この処理の詳細は、図45のフローチャートに示されている。すなわち、ステップS241において、レシーバ51の相互認証モジュール71(図26)は、通信部61を介して、サービスプロバイダ3-1の相互認証部45(図19)と相互認証し、相互認証できたとき、通信部61は、相互認証したサービスプロバイダ3-1から、サービスプロバイダセキュアコンテナ(図24)を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップS242に進む。

【0209】

ステップS242において、レシーバ51の通信部61は、ステップS241で相互認証したサービスプロバイダ3-1から、公開鍵証明書を受信する。

【0210】

ステップS243において、レシーバ51の復号/暗号化モジュール74は、ステップS241で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップS244に進む。

## 【0211】

ステップS244において、レシーバ51の記憶モジュール73に記憶されている基準情報51（図32）が、利用条件を満たすUCPと価格条件を満たすPTが選択され、表示制御部67を介して、図示せず表示部に表示される。ユーザFは、表示されたUCPおよびPTの内容を参照して、図示せぬ操作部を操作し、UCPの1つの利用内容を選択する。これにより、入力制御部68は、操作部から入力された、ユーザFの操作に対応する信号をSAM62に出力する。

## 【0212】

この例の場合、レシーバ51の基準情報51の「利用ポイント情報」には、図33に示したように、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイントであるとされてる。すなわち、この基準情報51によれば、コンテンツAに対応して設定されたUCPA、Bのうち、「利用条件10」の「ユーザ条件10」が”200ポイント以上”とされている、UCPAが選択される。また、基準情報51の「決済ユーザ情報」には、ユーザFは男性とされているので、PTA-1（図20（A））の「価格条件10」に設定された条件を満たす。その結果、UCPAに対応して作成されたPTA-1、PTA-2のうち、PTA-1が選択される。結局、UCPAおよびPTA-1の内容が、表示部に表示される。また、この例の場合、これにより、ユーザFが、UCPAの利用内容11（PTA-1の価格内容11）を選択したものとする。

## 【0213】

ステップS245において、レシーバ51のSAM62の課金処理モジュール72は、ステップS244で選択された、UCPAの「利用内容11」の内容（PTA-1の「価格内容11」の内容）に基づいて、UCSA（図28）および課金情報A（図30）を作成する。すなわち、この場合、コンテンツAは、料金が2000円で買い取り再生される。

## 【0214】

ステップS246において、サービスプロバイダセキュアコンテナ（図24）に含まれる、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、UCPA、PT-1、A-2、およびコンテンツプロバイダ2の署名が取り出され、HDD

52に出力され、記憶される。ステップS247において、復号／暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）を、記憶モジュール73に記憶されている配送用鍵Kdで復号する。

【0215】

ステップS248において、復号／暗号化ユニット74の暗号化ユニット93は、ステップS247で復号されたコンテンツ鍵KcoAを、記憶モジュール73に記憶されている保存用鍵Ksaveで暗号化する。

【0216】

ステップS249において、SAM62のデータ検査モジュール75は、ステップS248で保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSAが対応して記憶される、外部記憶部63の利用情報記憶部63A（図29）のブロックBPを検出する。この例の場合、利用情報記憶部63AのブロックBP-1が検出される。なお、図29の利用情報記憶部63Aにおいて、そのブロックBP-1の利用情報用メモリ領域RP-3にコンテンツ鍵KcoAおよびUCSAが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックBP-1の利用情報用メモリ領域RP-3は、空いており、所定の初期情報が記憶されているものとする。

【0217】

ステップS250において、レシーバ51のデータ検査モジュール75は、ステップS249で検出したブロックBP-1のデータ（利用情報用メモリ領域RP-1乃至RP-Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップS251において、データ検査モジュール75は、ステップS250で得られたハッシュ値と、記憶モジュール73に記憶されているブロックBP-1に対応する検査値HP-1（図31）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックBP-1のデータは改竄されていないので、ステップS252に進む。

【0218】

ステップ S 2 5 2 において、レシーバ 5 1 の SAM 6 2 は、利用情報（ステップ S 2 4 8 で、保存用鍵 K s a v e で暗号化されたコンテンツ鍵 K c o A、およびステップ S 2 4 5 で作成された UCSA（図 2 8））を、図 2 9 に示すように、利用情報記憶部 6 3 A（外部記憶部 6 3）のブロック BP-1 の利用情報用メモリ領域 RP-3 に記憶させる。

## 【0219】

ステップ S 2 5 3 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、ステップ S 2 5 2 で利用情報が記憶された利用情報用メモリ領域 RP-3 が属する、利用情報記憶部 6 3 A のブロック BP-1 のデータにハッシュ関数を適用し、ハッシュ値を算出し、ステップ S 2 5 4 において、記憶モジュール 7 3 に記憶されている検査値 HP-1 に上書きする。ステップ S 2 5 5 において、課金処理モジュール 7 2 は、ステップ S 2 4 5 で作成した課金情報 A を記憶モジュール 7 3 に記憶させ、処理は終了する。

## 【0220】

ステップ S 2 5 1 において、算出されたハッシュ値と検査値 HP-1 とが一致しないと判定された場合、ブロック BP-1 のデータは改竄されているので、手続きは、ステップ S 2 5 6 に進み、データ検査モジュール 7 5 は、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック BP を調べたか否かを判定し、外部記憶部 6 3 の全てのブロック BP を調べていないと判定した場合、ステップ S 2 5 7 に進み、利用情報記憶部 6 3 A の、調べていない（空きを有する他の）ブロック BP を検索し、ステップ S 2 5 0 に戻り、それ以降の処理が実行される。

## 【0221】

ステップ S 2 5 6 において、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック BP が調べられたと判定された場合、利用情報を記憶できるブロック BP（利用情報用メモリ領域 RP）は存在しないので、処理は終了する。

## 【0222】

このように、サービスプロバイダセキュアコンテナが、レシーバ 5 1 により受信されると、処理は終了し、図 3 8 のステップ S 1 5 に進む。

## 【0223】

ステップ S 1 5 において、供給されたコンテンツ A が、レシーバ 5 1 において利用される。なお、この例の場合、図 4 5 のステップ S 2 2 4 で選択された UCP A の利用内容 1 1 によれば、コンテンツ A は、再生して利用される。そこで、ここでは、コンテンツ A の再生処理について説明する。この再生処理の詳細は、図 4 6 のフローチャートに示されている。

#### 【0 2 2 4】

ステップ S 2 6 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、図 4 5 のステップ S 2 5 2 で、コンテンツ鍵 K c o A（保存用鍵 K s a v e で暗号化されている）および UCS A が記憶された利用情報用メモリ領域 R P-3 が属する、外部記憶部 6 3 の利用情報記憶部 6 3 A のブロック B P-1 のデータにハッシュ関数を適用してハッシュ値を算出する。

#### 【0 2 2 5】

ステップ S 2 6 2 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、ステップ S 2 6 1 において算出したハッシュ値が、図 4 5 のステップ S 2 5 3 で算出し、ステップ S 2 5 4 で記憶モジュール 7 3 に記憶させたハッシュ値（検査値 H P-1）と一致するか否かを判定し、一致すると判定した場合、ブロック B P-1 のデータは改竄されていないので、ステップ S 2 6 3 に進む。

#### 【0 2 2 6】

ステップ S 2 6 3 において、UCS A（図 2 8）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツ A が利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされている UCS においては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされている UCS においては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が 0 回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能

回数が0回であるとき、利用不可と判定される。

【0227】

なお、UCSAの「利用内容」の「形式」は、“買い取り再生”とされているので、この場合、コンテンツAは、買い取られ、制限なしに再生される。すなわち、UCSAの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップS263において、コンテンツAが利用可能であると判定され、ステップS264に進む。

【0228】

ステップS264において、レシーバ51の課金モジュール72は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

【0229】

次に、ステップS265において、レシーバ51のSAM62は、ステップS264で更新されたUCSA（実際は、更新されていない）を、外部記憶部63の利用情報記憶部63AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS266において、データ検査モジュール75は、ステップS265でUCSAが記憶された、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール73に記憶されている検査値HP-1に上書きする。

【0230】

ステップS267において、SAM62の相互認証モジュール71と、伸張部64の相互認証モジュール101は、相互認証し、SAM62および伸張部64は、一時鍵Ktempを共有する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、R3、またはその組み合わせが、一時鍵Ktempとして用いられる。



## 【0231】

ステップS268において、復号／暗号化モジュール74の復号ユニット91は、図45のステップS252で外部記憶部63の利用情報記憶部63AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）を、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。

## 【0232】

次に、ステップS269において、復号／暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵KcoAを一時鍵Ktempで暗号化する。ステップS270において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵KcoAを伸張部64に送信する。

## 【0233】

ステップS271において、伸張部64の復号モジュール102は、コンテンツ鍵KcoAを一時鍵Ktempで復号する。ステップS272において、伸張部64は、インタフェース66を介して、HDD52に記録されたコンテンツA（コンテンツ鍵Kcoで暗号化されている）を受け取る。ステップS273において、伸張部64の復号モジュール103は、コンテンツA（コンテンツ鍵Kcoで暗号化されている）をコンテンツ鍵KcoAで復号する。

## 【0234】

ステップS274において、伸張部64の伸張モジュール104は、復号されたコンテンツAをATRAC2などの所定の方式で伸張する。ステップS275において、伸張部64のウォータマーク付加モジュール105は、伸張されたコンテンツAにレシーバ51を特定する所定のウォータマーク（電子透かし）を挿入する。ステップS276において、コンテンツAは、図示せぬスピーカなどに出力され、処理は終了する。

## 【0235】

ステップS262において、ステップS261において算出されたハッシュ値が、レシーバ51の記憶モジュール73に記憶されたハッシュ値と一致しないと判定された場合、またはステップS263において、コンテンツが利用不可と判

定された場合、ステップS277において、SAM62は、表示制御部67を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

#### 【0236】

このようにして、レシーバ51において、コンテンツAが再生（利用）されたとき、処理は終了し、図38の処理も終了する。

#### 【0237】

次に、レシーバ51の課金が決済される場合の処理手順を、図47のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵Kdのバージョンが古くなり、例えば、図45のステップS247で、コンテンツ鍵Kco（配送用鍵Kdで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

#### 【0238】

ステップS301において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図40乃至図42を参照して説明した場合と同様の処理であるので、その説明は省略する。

#### 【0239】

次に、ステップS302において、レシーバ51のSAM62は、EMDサービスセンタ1のユーザ管理部18（図3）に証明書を送信する。ステップS303において、レシーバ51のSAM62は、記憶モジュール73に記憶されている課金情報を、ステップS301で、EMDサービスセンタ1と共有した一時鍵Ktempで暗号化し、配送用鍵Kdのバージョン、HDD52に記憶されてる、対応するUCPとPT、並びに登録リストとともに、EMDサービスセンタ1に送信する。

#### 【0240】

ステップS304において、EMDサービスセンタ1のユーザ管理部18は、ステップS303で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に”停

止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

#### 【0241】

ステップS305において、EMDサービスセンタ1の課金請求部19は、ステップS303で受信された課金情報を解析し、ユーザ（例えば、ユーザF）の支払い金額を算出する処理等を行う。次に、ステップS306において、ユーザ管理部18は、ステップS305における処理により、決済が成功したか否かを確認する。

#### 【0242】

次に、ステップS307において、EMDサービスセンタ1のユーザ管理部18は、ステップS304における確認結果、およびステップS306における確認結果に基づいて、レシーバ51の登録条件を設定し、それに署名を付して、レシーバ51の登録リストを作成する。

#### 【0243】

例えば、ステップS304で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS306で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

#### 【0244】

次に、ステップS308に進み、EMDサービスセンタ1のユーザ管理部18は、最新バージョンの配送用鍵Kd（3月分の最新バージョンの配送用鍵Kd）およびステップS307で作成された登録リストを、一時鍵Ktempで暗号化し、レシーバ51に送信する。なお、登録リストには、署名が付されているので、暗号化しなくてもよい。

#### 【0245】

ステップS309において、レシーバ51のSAM62は、EMDサービスセンタ1から送信された配送用鍵Kdおよび登録リスト情報を、通信部61を介して受信

し、復号した後、配送用鍵 K d を記憶モジュール 7 3 に記憶させ、登録リストを HDD 5 2 に記憶させる。このとき、記憶モジュール 7 3 に記憶されていた課金情報は消去され、登録リストおよび配送用鍵 K d が更新される。

#### 【0 2 4 6】

次に、レシーバ 5 1 からレシーバ 2 0 1 に、コンテンツ A が管理移動される場合の処理手順を、図 4 8 のフローチャートを参照して説明する。

#### 【0 2 4 7】

ステップ S 4 0 1 において、レシーバ 5 1 とレシーバ 2 0 1 との間で、相互認証が行われる。この相互認証は、図 4 0 乃至図 4 2 を参照して説明した同様であるので、その説明は省略する。

#### 【0 2 4 8】

次に、ステップ S 4 0 2 において、レシーバ 5 1（管理移動元の機器）の SAM 6 2 およびレシーバ 2 0 1（管理移動先の機器の SAM）の SAM 2 1 2 のそれぞれは、各自が保持する登録リストを参照し、コンテンツの管理移動が可能であるか否かを確認する。具体的には、管理移動元の機器の SAM（レシーバ 5 1 の SAM 6 2）は、自分の登録リストに、管理移動先の機器（レシーバ 2 0 1）の登録条件が設定されているか否かを確認し、それが設定されている場合、コンテンツの管理移動が可能であると判定する。同様に、管理移動先の機器の SAM（レシーバ 2 0 1 の SAM 2 1 2）も、自分の登録リストに、管理移動元の機器（レシーバ 5 1）の登録条件が設定されているか否かを確認し、それが設定されている場合、コンテンツの管理移動が可能であると判定する。いずれか一方においても、コンテンツの管理移動が可能でないと判定された場合、処理は終了するが、この例の場合、それぞれの登録条件は、それぞれの登録リストに設定されているので、両者において、コンテンツの管理移動が可能であると判定され、ステップ S 4 0 3 に進む。

#### 【0 2 4 9】

次に、ステップ S 4 0 3 において、レシーバ 2 0 1 のデータ検査モジュール 2 5 は、後述するステップ S 4 1 4 で受信する移動情報（コンテンツ鍵 K c o A（保存用鍵 K s a v e で暗号化されている）、コンテンツ A の ID、および SAM 6

2のID)を記憶する、外部記憶部213の移動情報記憶部213A(図36)のブロックBMを検出する。この例の場合、ステップS403において、ブロックBM-1が検出される。なお、図36の利用情報記憶部213Aにおいて、そのブロックBM-1の移動情報用メモリ領域RM-1には、コンテンツ鍵KcoA、コンテンツAのID、およびSAM62のIDが記憶されているように示されているが、この例の場合、この時点において、その移動情報用メモリ領域RM-1は、空いているものとする。

#### 【0250】

ステップS404において、レシーバ201のデータ検査モジュール225は、ステップS403で検出したブロックBM-1のデータが改竄されているか否かを判定する。具体的には、データ検査モジュール225は、ブロックBM-1に記憶されているデータにハッシュ関数を適用してハッシュ値を算出する。そしてデータ検査モジュール225は、算出したハッシュ値と、記憶モジュール223に記憶される、ブロックBM-1に対応する検査値HM-1が一致するか否かを判定し、一致していると判定した場合、すなわち、ブロックBM-1が改竄されていない場合、ステップS405に進む。

#### 【0251】

ステップS405において、レシーバ201のSAM212は、コンテンツの管理移動が可能であることを示す信号を通信部215を介して、レシーバ51に送信する。

#### 【0252】

ステップS406において、レシーバ51が、レシーバ201から、コンテンツの管理移動が可能であることを示す信号を受信すると、レシーバ51のデータ検査モジュール75は、管理移動されるコンテンツAに対応するコンテンツ鍵KcoAが記憶されている、外部記憶部63の利用情報記憶部63A(図29)のブロックBP-1を検出する。

#### 【0253】

ステップS407において、レシーバ51のデータ検査モジュール75は、ステップS406で検出したブロックBP-1のデータが改竄されているか否かを

判定する。具体的には、データ検査モジュール75は、ブロックBP-1に記憶されているデータの全てにハッシュ関数を適用してハッシュ値を算出する。そしてデータ検査モジュール75は、算出したハッシュ値が、記憶モジュール73に記憶されている、ブロックBP-1に対応する検査値HP-1（図45のステップS253で算出され、ステップS254で記憶されたハッシュ値）と一致するかどうかを判定し、一致すると判定した場合、すなわち、ブロックBP-1のデータが改竄されていない場合、ステップS408に進む。

## 【0254】

ステップS408において、レシーバ51のSAM62は、ステップS406で検出された、外部記憶部63の利用情報記憶部63のブロックBP-1（利用情報用メモリ領域RP-3）に記憶されているUCSA（図28）の「利用内容」の「形式」を参照し、コンテンツの利用形式が”買い取り再生”であるかどうかを判定する。UCSAの場合のように、その「利用内容」の「形式」が、”買い取り再生”とされているとき、コンテンツの利用形式が”買い取り再生”であると判定され、ステップS409に進む。

## 【0255】

ステップS409において、レシーバ51のSAM62は、UCSAの「利用内容」の「管理移動状態情報」に設定されている管理移動先の機器のIDが、自分自身のIDとされているかどうか、すなわち、コンテンツが管理移動されているかどうかを判定し、コンテンツが管理移動されていないと判定した場合、ステップS410に進む。

## 【0256】

ステップS410において、レシーバ51のSAM62は、今回のコンテンツAの管理移動先の機器であるレシーバ201のSAM212のIDを、UCSAの「利用内容」の「管理移動状態情報」に管理移動先の機器のIDとして設定する。次に、ステップS411において、レシーバ51のデータ検査モジュール75は、ステップS410で、「利用内容」の「管理移動状態情報」の内容が変更（管理移動先のIDが、SAM62のIDからSAM212のIDに変更）されたUCSAが記憶されているブロックBP-1のデータにハッシュ関数を適用しハッシュ値を算出し、それを

、ステップS412において、記憶モジュール73に記憶されている、ブロックBP-1に対応するハッシュ値HP-1に上書きする。

【0257】

次に、ステップS413において、レシーバ51のSAM62は、外部記憶部63の利用情報記憶部63AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されているコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）を保存用鍵Ksaveで復号し、ステップS401でレシーバ201と共有した一時鍵Ktempで暗号化した後、自分自身のID（SAM62のID）およびUCSAの「コンテンツのID」に設定されているコンテンツAのIDとともに、レシーバ201に送信する。なお、この処理が実行されるタイミングで、HDD52に記憶されているコンテンツAは、レシーバ201に送信される。

【0258】

ステップS414において、レシーバ51から送信されてきたコンテンツ鍵KocA（一時鍵Ktempで暗号化されている）、SAM62のID、およびコンテンツAのIDがレシーバ201により受信されると、ステップS415において、レシーバ201のSAM212は、受信されたコンテンツ鍵KcoA（一時鍵Ktempで暗号化されている）を一時鍵Ktempで復号した後、自分自身が保持している保存用鍵Ksaveで再度暗号化して、それを、同様にSAM62のID、コンテンツAのID、および自分自身のID（SAM212のID）とともに、ステップS403で検出した、外部記憶部213の移動情報記憶部213AのブロックBM-1の移動情報用メモリ領域RM-1に、図36で示したように記憶させる。

【0259】

次に、ステップS416において、レシーバ201のSAM212は、ステップS415で移動情報が記憶された移動情報記憶部213AのブロックBM-1のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール223に記憶されている検査値HM-1に上書きする。

【0260】

ステップS417において、レシーバ51から供給されたコンテンツAがHDD202に記憶される。

## 【0261】

ステップS404で外部記憶部213の移動情報記憶部213AのブロックB M-1のデータが、またはステップS407で外部記憶部63の利用情報記憶部63AのブロックBP-1のデータが改竄されていると判定された場合、処理は終了する。すなわち、移動情報が記憶されるメモリ領域がまたは、利用情報が改竄されている場合（正確には、改竄されている恐れがある場合）、コンテンツの管理移動は行われぬ。

## 【0262】

ステップS407で、コンテンツAの利用形式が”買い取り”ではないと判定された場合、またはステップS408で、コンテンツAが管理移動されていると判定された場合も、処理は終了する。すなわち、コンテンツを買い取って再生する利用形式においてのみ、コンテンツの管理移動が行われる（許可される）。また、コンテンツが管理移動されている間は、さらに、そのコンテンツを管理移動することはできない（許可されない）。

## 【0263】

次に、上述した処理により、レシーバ201にコンテンツAが管理移動されている状態において、今度は、レシーバ51が、コンテンツAを戻す（管理移動を解除する）場合の処理手順を、図49のフローチャートを参照して説明する。

## 【0264】

ステップS431において、レシーバ51とレシーバ201との間で、相互認証が行われる。この相互認証は、図40乃至図42を参照して説明した場合と同様であるので、その説明は省略する。次に、ステップS432において、レシーバ51（管理移動元の機器）のSAM62およびレシーバ201（管理移動先の機器のSAM）のSAM212のそれぞれは、各自が保持する登録リストを参照し、管理移動の解除が可能であることを確認する。なお、ここでの具体的な処理は、図48のステップS402における場合と同様であるので、その説明は省略する。

## 【0265】

ステップS433において、レシーバ51のデータ検査モジュール75は、管理移動されているコンテンツA（コンテンツ鍵KcoAで暗号化されている）に



対応するコンテンツ鍵Kc o Aが記憶されている外部記憶部63の利用情報記憶部63A(図29)のブロックBPを検出する。この例の場合、ブロックBP-1が検出される。

## 【0266】

次に、ステップS434において、レシーバ51のデータ検査モジュール75は、ステップS433で検出したブロックBP-1のデータが改竄されているか否かを判定する。ここでの具体的な処理は、図48のステップS407における場合と同様であるので、その説明は省略する。

## 【0267】

ステップS434で、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータが改竄されていないと判定された場合、ステップS435に進み、レシーバ51のSAM62は、外部記憶部63の利用情報記憶部63AのブロックBP-1に記憶されているUCSA(図28)から、コンテンツAのIDおよびSAM62のIDを読み出し、それらを、管理移動の解除を要求する所定の信号(以下、管理移動解除要求信号と称する)とともに、レシーバ201に送信する。

## 【0268】

ステップS436において、レシーバ51から送信されてきた、コンテンツAのID、SAM62のID、および管理移動解除要求信号が受信されると、ステップS437において、レシーバ201のSAM212は、受信されたコンテンツAのIDが記憶されている、外部記憶部213の移動情報記憶部213AのブロックBMを検出する。この例の場合、ブロックBM-1が検出される。

## 【0269】

ステップS438において、レシーバ201のSAM212は、外部記憶部213の移動情報記憶部213AのブロックBM-1(移動情報用メモリ領域RM-1)に、ステップS436で受信されたSAM62のIDが記憶されているか否かを判定し、記憶されていると判定した場合、ステップS439に進む。この例の場合、ブロックBM-1の移動情報用メモリ領域RM-1には、SAM62のIDが記憶されているので、ステップS439に進む。

## 【0270】

ステップS439において、レシーバ201のSAM212は、SAM62のIDが記憶されてるブロックBM-1が改竄されているか否かを判定する。ここでの具体的な処理は、図48のステップS404における場合と同様であるので、その説明は省略する。ステップS439において、ブロックBM-1が改竄されていないと判定された場合、ステップS440に進む。

## 【0271】

ステップS440において、レシーバ201のSAM212は、外部記憶部213の移動情報記憶部213AのブロックBM-1（移動情報用メモリ領域RM-1）に、ステップS436で受信されたコンテンツのIDが記憶されているか否かを判定し、記憶されていると判定した場合、ステップS441に進む。この例の場合、ブロックBM-1の移動情報用メモリ領域RM-1には、コンテンツAのIDが記憶されているので、ステップS441に進む。

## 【0272】

ステップS441において、レシーバ201のSAM212は、外部記憶部213の移動情報記憶部213AのブロックBM-1（移動情報用メモリ領域RM-1）に記憶されている移動情報を削除する。これにより、ブロックBM-1の移動情報用メモリ領域RM-1には、所定の初期情報が記憶される。なお、この処理が実行されるタイミングで、HDD202に記憶されているコンテンツAも削除される。

## 【0273】

次に、ステップS442において、レシーバ201のデータ検査モジュール225は、ステップS441で移動情報が削除された移動情報用メモリ領域RM-1が属するブロックBM-1のデータにハッシュ関数を適用してハッシュ値を算出し、それを、記憶モジュール223に記憶されている、ブロックBM-1に対応するハッシュ値HM-1に上書きする。

## 【0274】

ステップS443において、レシーバ201のSAM212は、コンテンツの管理移動が解除されたことを示す信号（以下、管理移動解除信号と称する）を、レシーバ51に送信する。

## 【0275】

ステップS444において、レシーバ201からの管理移動解除信号が受信されると、レシーバ51のSAM62は、自分自身のIDを、UCSAの「利用内容」の「管理移動状態情報」に、管理移動先の機器のIDとして記憶させる（管理移動元の機器のIDは、SAM62のIDとされている）。

## 【0276】

次に、ステップS445において、レシーバ51のデータ検査モジュール75は、ステップS444で、「利用内容」の管理移動状態情報の内容が変更（管理移動先のIDが、SAM212のIDからSAM62のIDに変更）されたUCSAが記憶されているブロックBP-1のデータにハッシュ関数を適用してハッシュ値を算出し、それを、ステップS446において、記憶モジュール73に記憶されている、ブロックBP-1に対応する検査値HP-1に上書きする。

## 【0277】

以上のようにして、コンテンツの管理移動が解除されるとき、管理移動先の機器である、レシーバ201から移動情報が削除されるようにしたので、レシーバ201においてコンテンツAは利用されないようになる。またこのとき、UCSAの「利用内容」の「管理移動状態情報」に、管理移動元の機器のSAMのID（レシーバ51のSAM62）のIDが、管理移動先の機器のIDとしても設定されるようにしたので、レシーバ51は、コンテンツAの管理移動を行うことができるようになる。

## 【0278】

なお、以上においては、コンテンツの利用形式が”買い取り再生”である場合にのみ管理移動が可能となる場合を例として説明したが、利用形式が”期間制限再生”である場合においても管理移動が可能となるようにすることもできる。

## 【0279】

また、以上においては、管理移動が解除される場合、レシーバ51がレシーバ201に管理移動解除要求信号を送信する場合（レシーバ51が管理移動の解除を要求する場合）を例として説明したが、レシーバ201が管理移動の解除を要求することもできる。

## 【0280】

さらに、以上においては、SAM 62 の公開鍵  $K_{pu}$  および SAM 62 の証明書がレシーバ 51 の記憶モジュール 73 が記憶されているものとしたが、HDD 52 に記憶させておくこともできる。同様に、SAM 212 の公開鍵  $K_{pu}$  および SAM 212 の証明書も、HDD 202 に記憶させておくこともできる。

## 【0281】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であれば MPEG (Moving Picture Experts Group) などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

## 【0282】

また、共通鍵暗号は、ブロック暗号である DES を使用して説明したが、NTT (商標) が提案する FEAL、IDEA (International Data Encryption Algorithm)、または 1 ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

## 【0283】

さらに、コンテンツおよびコンテンツ鍵  $K_{co}$  の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

## 【0284】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

## 【0285】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

## 【0286】

## 【発明の効果】

請求項 1 に記載の情報処理装置、請求項 3 に記載の情報処理方法、および請求項 4 に記載の提供媒体によれば、移動状態情報が、価値情報の移動が行われてい

ないことを示しているとき、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更し、制御信号に対する応答信号が受信されたとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更するようにしたので、著作権の保護を確保しながら、価値情報の移動を行うことができる。

【0287】

請求項5に記載の情報処理装置、請求項7に記載の情報処理方法、および請求項8に記載の提供媒体によれば、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信し、所定の制御信号を受信したとき、記憶された移動情報を削除するようにしたので、著作権の保護を確保しながら、移動された価値情報を利用することができる。

【図面の簡単な説明】

【図1】

EMDシステムを説明する図である。

【図2】

EMDシステムにおける、主な情報の流れを説明する図である。

【図3】

EMDサービスセンタ1の機能的構成を示すブロック図である。

【図4】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する図である。

【図5】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の図である。

【図6】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の図である。

【図7】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の図である。

【図8】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の図である。

【図9】

システム登録情報を説明する図である。

【図 10】

利用ポイント情報を説明する図である。

【図 11】

コンテンツプロバイダ 2 の機能的構成例を示すブロック図である。

【図 12】

UCP を説明する図である。

【図 13】

コンテンツの管理移動を説明する図である。

【図 14】

第 1 世代複製を説明する図である。

【図 15】

サービスコードおよびコンディションコードのコード値の例を示す図である。

【図 16】

UCP の利用条件として設定されたコード値の例を示す図である。

【図 17】

コンテンツプロバイダセキュアコンテナの例を示す図である。

【図 18】

コンテンツプロバイダ 2 の証明書の例を示す図である。

【図 19】

サービスプロバイダ 3 の機能の構成を示すブロック図である。

【図 20】

PT の例を示す図である。

【図 21】

PT の価格条件として設定されたコード値の例を示す図である。

【図 22】

他の PT の例を示す図である。

【図 23】

他の PT の価格条件として設定されたコード値の例を示す図である。

【図 2 4】

サービスプロバイダセキュアコンテナの例を示す図である。

【図 2 5】

サービスプロバイダ 3 の証明書の例を示す図である。

【図 2 6】

ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

【図 2 7】

レシーバ 5 1 の SAM 6 2 の証明書の例を示す図である。

【図 2 8】

UCS の例を示す図である。

【図 2 9】

レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する図である。

【図 3 0】

課金情報の例を示す図である。

【図 3 1】

レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図である。

【図 3 2】

基準情報 5 1 を説明する図である。

【図 3 3】

基準情報 5 1 の利用ポイント情報の例を示す図である。

【図 3 4】

登録リストの例を示す図である。

【図 3 5】

ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

【図 3 6】

レシーバ 2 0 1 の外部記憶部 2 1 3 の移動情報記憶部 2 1 3 A の内部を説明す

る図である。

【図 3 7】

レシーバ 2 0 1 の記憶モジュール 2 2 3 に記憶されている情報を示す図である。

【図 3 8】

コンテンツの利用処理を説明するフローチャートである。

【図 3 9】

EMDサービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 4 0】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 4 1】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 4 2】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 4 3】

コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 4 4】

サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 4 5】

レシーバ 5 1 がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

【図 4 6】

レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。



【図47】

課金を決済する処理を説明するフローチャートである。

【図48】

コンテンツを管理移動する処理を説明するフローチャートである。

【図49】

コンテンツの管理移動を終了する処理を説明するフローチャートである。

【符号の説明】

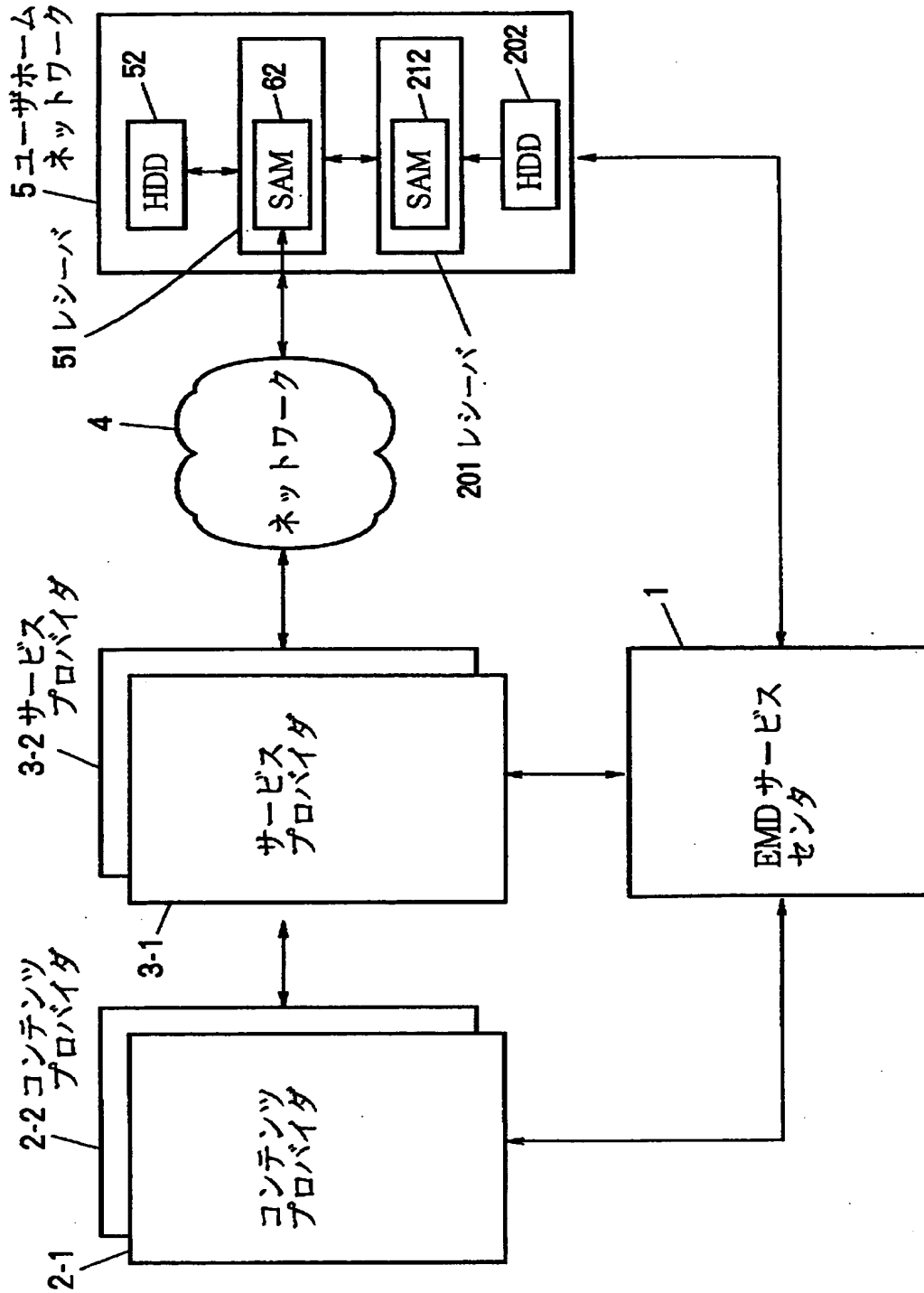
1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 11 サービスプロバイダ管理部, 12 コンテンツプロバイダ管理部, 13 著作権管理部, 14 鍵サーバ, 15 経歴データ管理部, 16 利益分配部, 17 相互認証部, 18 ユーザ管理部, 19 課金請求部, 20 出納部, 21 監査部, 31 コンテンツサーバ, 32 ウォータマーク付加部, 33 圧縮部, 34 暗号化部, 35 乱数発生部, 36 暗号化部, 37 ポリシー記憶部, 38 セキュアコンテナ作成部, 39 相互認証部, 41 コンテンツサーバ, 42 値付け部, 43 ポリシー記憶部, 44 セキュアコンテナ作成部, 45 相互認証部, 51 レシーバ, 52 HDD, 61 通信部, 62 SAM, 63 外部記憶部, 64 伸張部, 65 通信部, 66 インタフェース, 67 表示制御部, 68 入力制御部, 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジュール, 74 復号/暗号化モジュール, 75 データ検査モジュール, 91 復号ユニット, 92 乱数発生ユニット, 93 暗号化ユニット, 101 相互認証モジュール, 102 復号モジュール, 103 復号モジュール, 104 伸張モジュール, 105 ウォータマーク付加モジュール, 201 レシーバ, 202 HDD, 211 通信部, 212 SAM, 213 外部記憶部, 214 伸張部, 215 通信部, 216 インタフェース, 217 表示制御部, 218 入力制御部, 221 相互認証モジュール, 222 課金処理モジュール, 223 記憶モジュール, 224 復号/暗号化モジュール, 225 データ検査モジュール, 231

復号ユニット, 232 乱数発生ユニット, 233 暗号化ユニット, 2  
41 相互認証モジュール, 242 復号モジュール, 243 復号モジュ  
ール, 244 伸張モジュール, 245 ウォータマーク付加モジュール

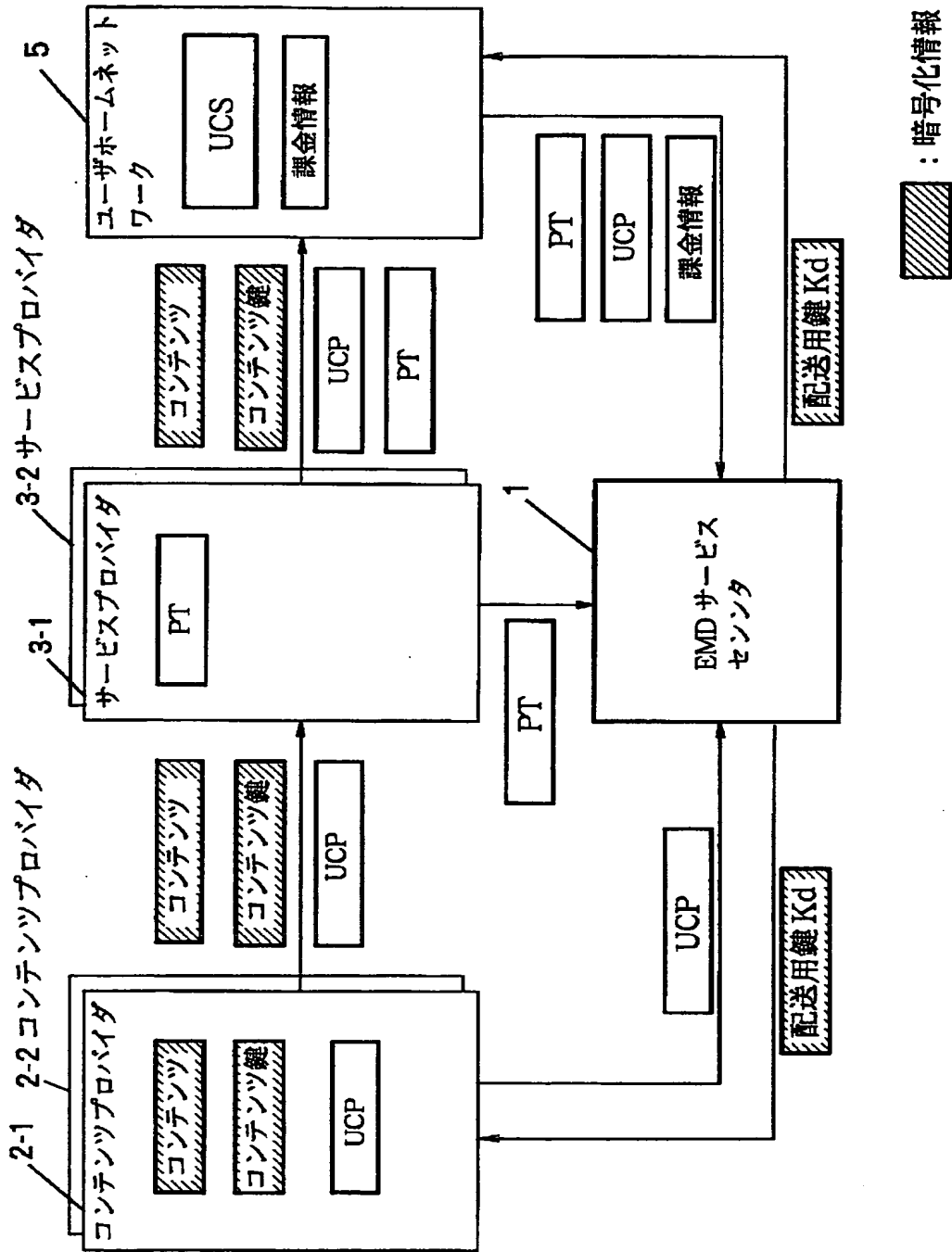
【書類名】

図面

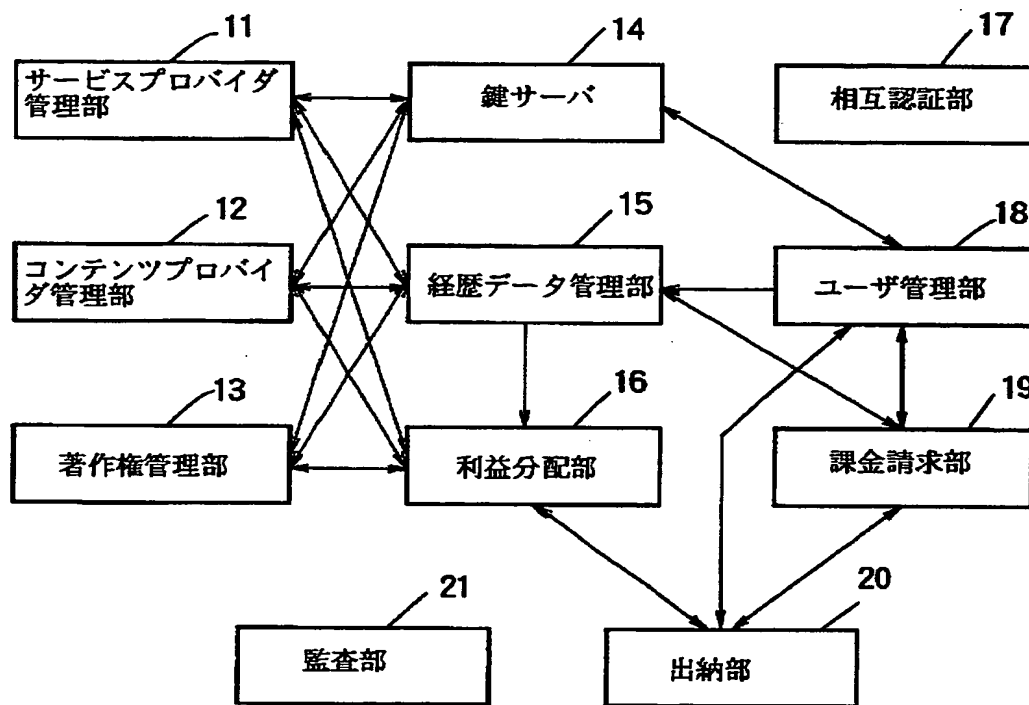
【図 1】



【図 2】

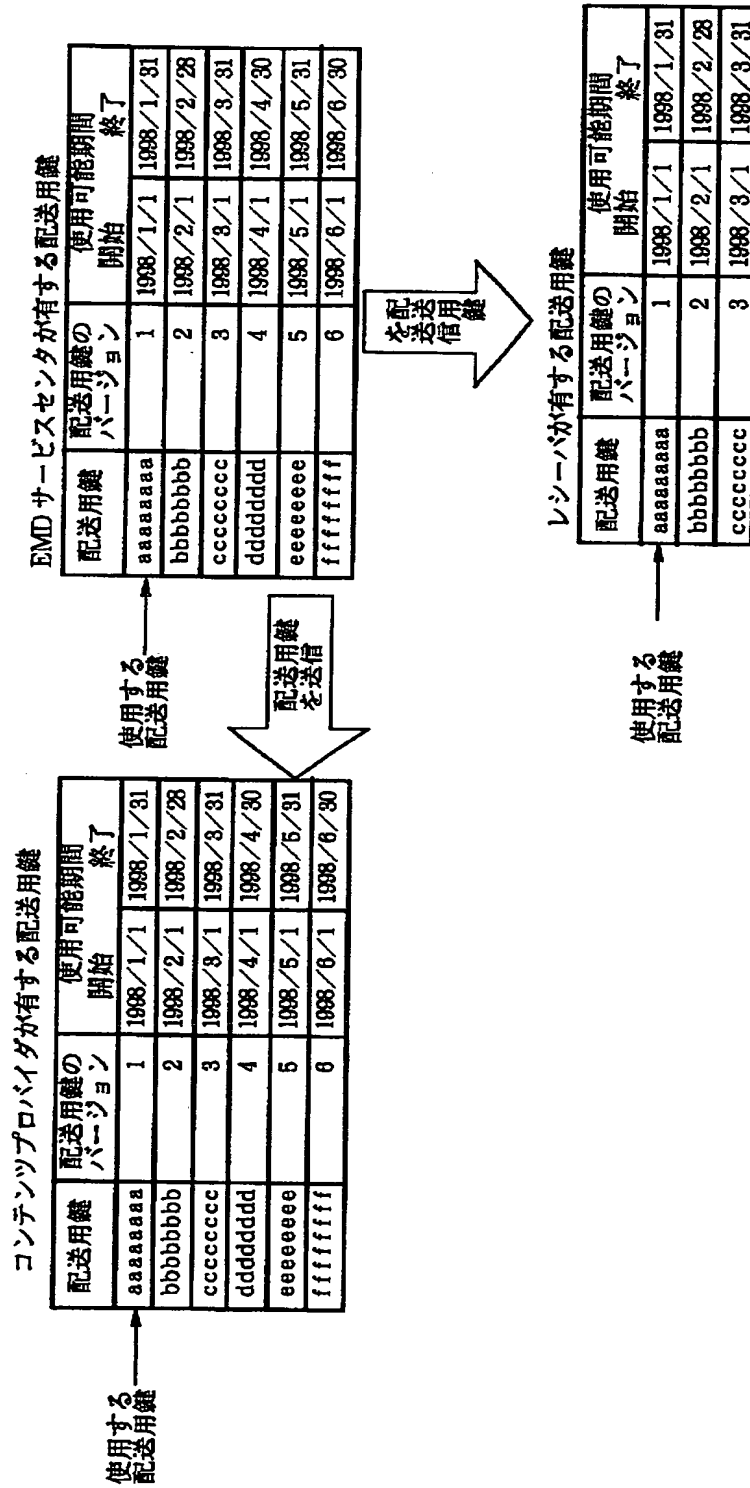


【図 3】

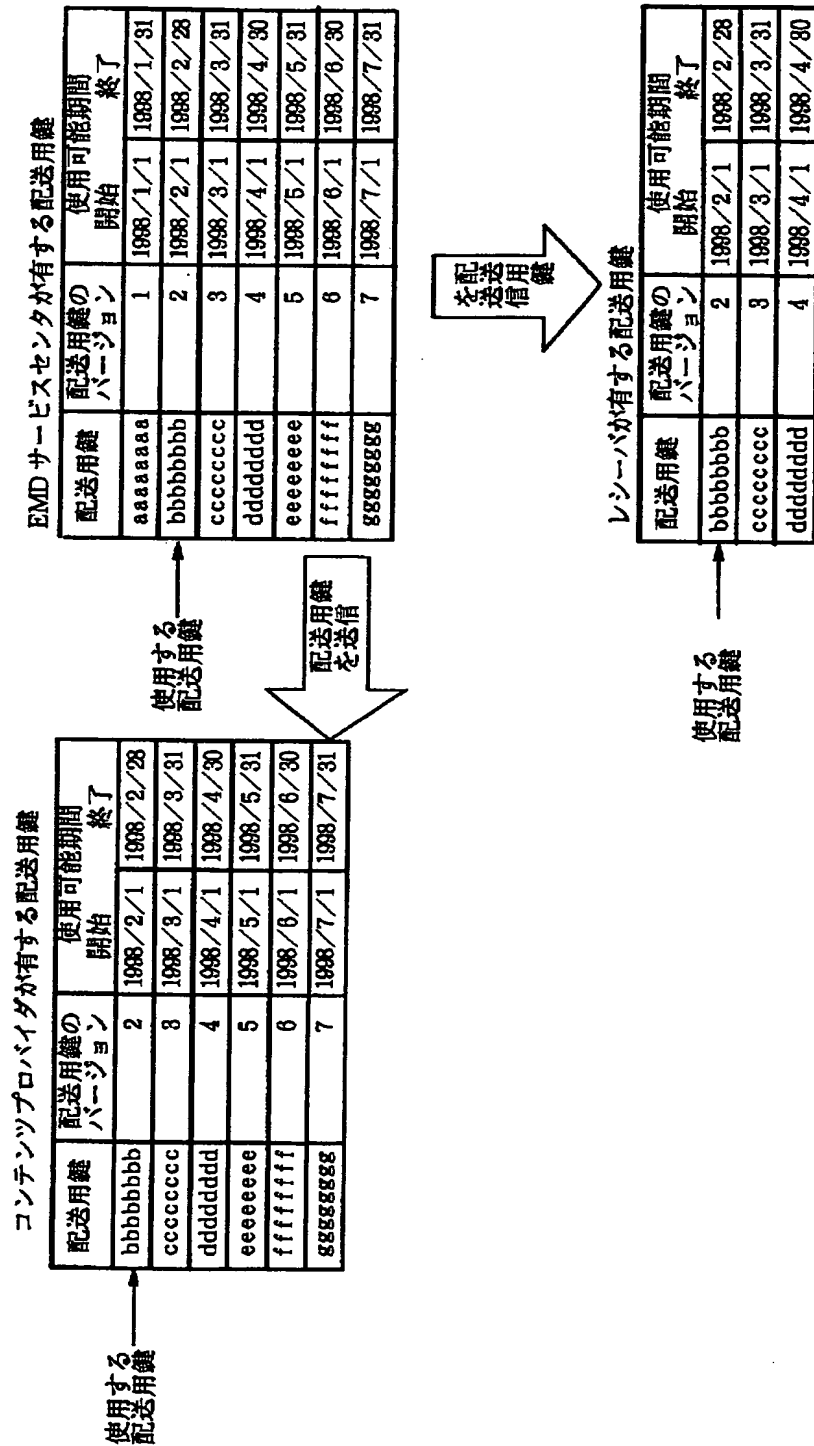


EMD サービスセンタ 1

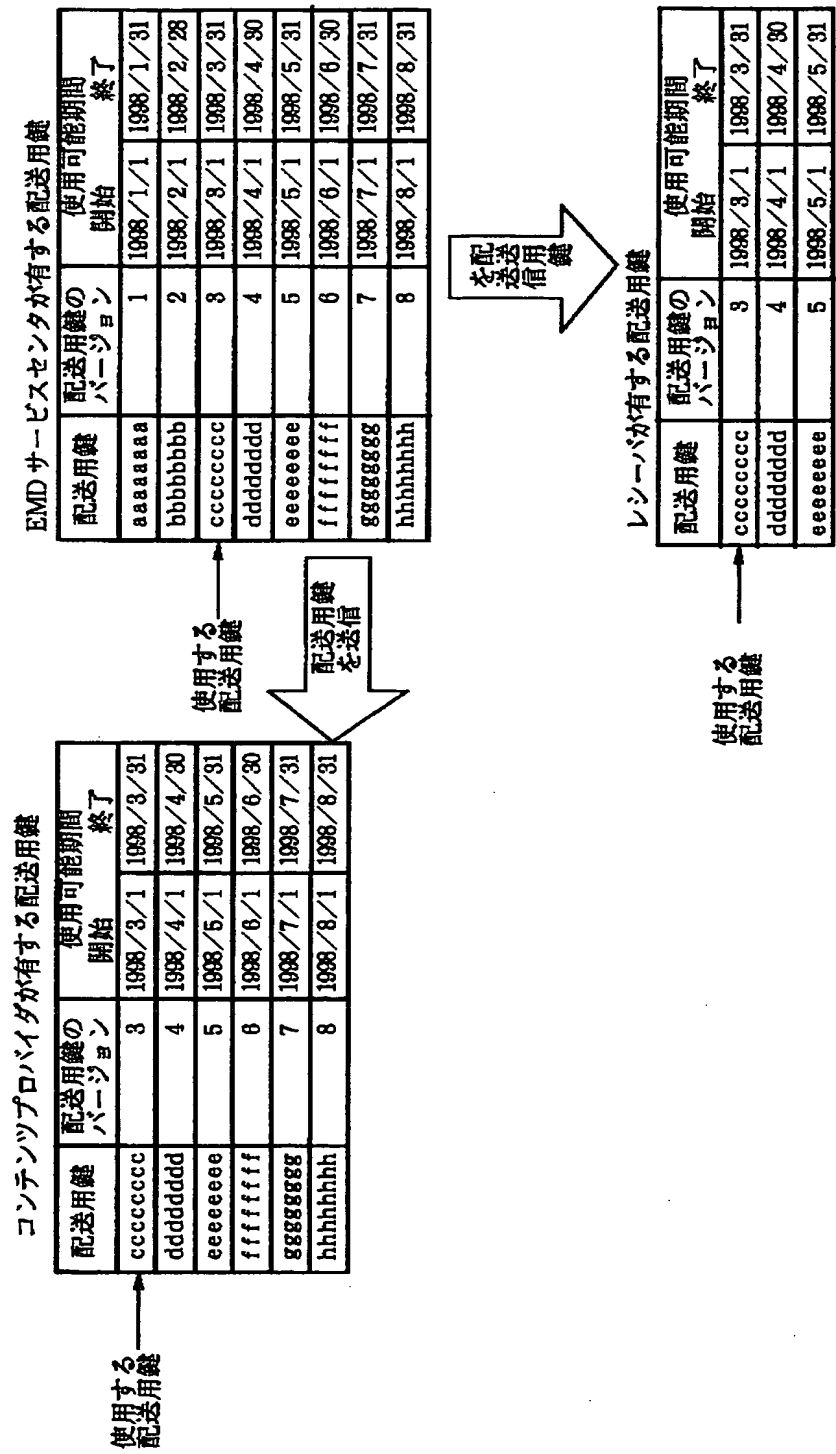
【図 4】



【図 5】

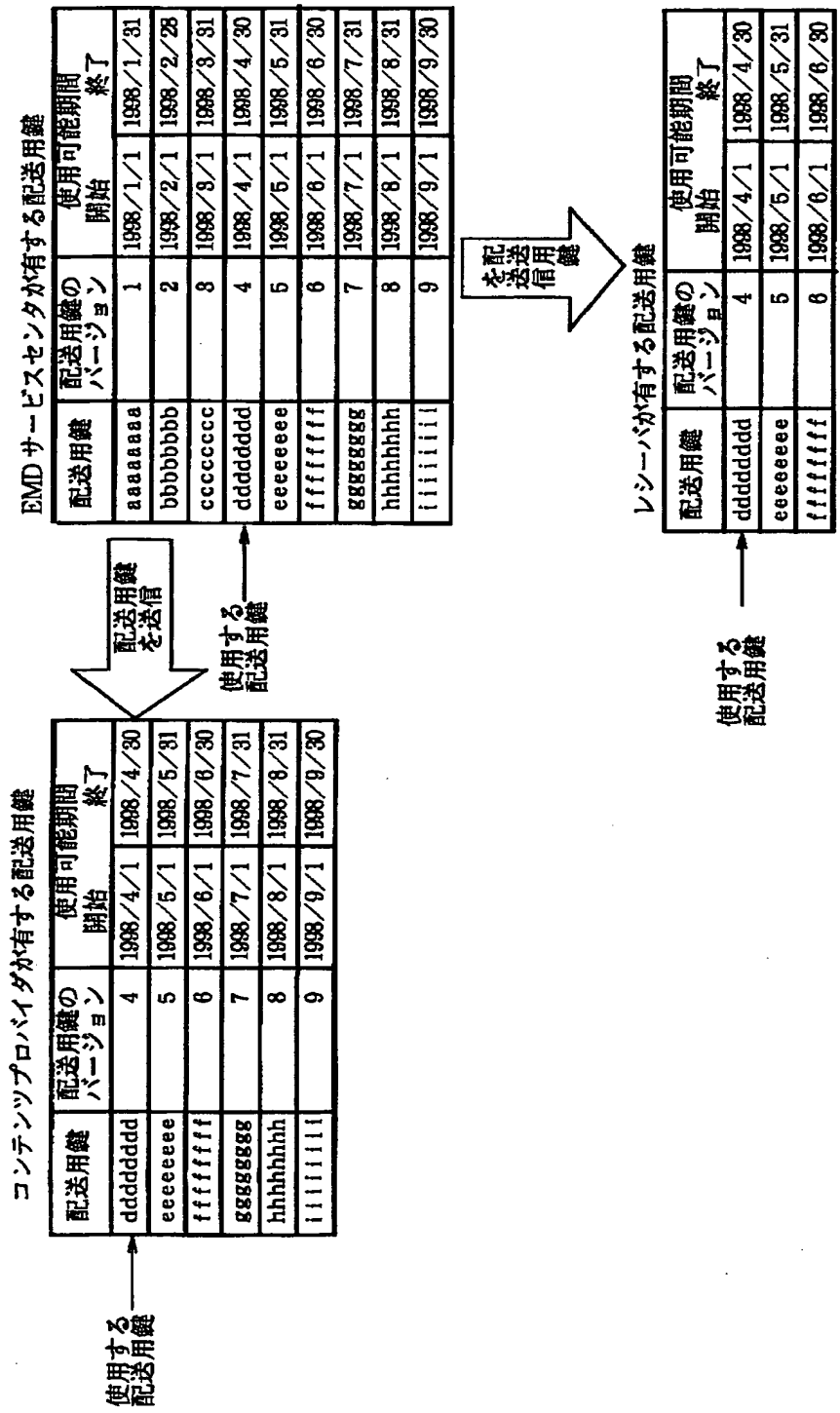


【図 6】





【図 7】



【図 8】

配送用鍵	配送用鍵の バージョン	使用可能期間 開始 終了
aaaaaaaa	1	1998/1/1 1998/1/31

仮配送用鍵 Kd

【図 9】

SAM の ID		SAM62 の ID	SAM212 の ID
機器番号		レシーバ 51 の 機器番号(100 番)	レシーバ 201 の 機器番号(100 番)
決済 ID		ユーザ F の決済 ID	ユーザ A の決済 ID
決済 ユーザ 情報	氏名	ユーザ F の氏名	ユーザ A の氏名
	住所	ユーザ F の住所	ユーザ A の住所
	電話番号	ユーザ F の電話番号	ユーザ A の電話番号
	決済機関情報	ユーザ F の決済情報	ユーザ A の決済情報
	生年月日	ユーザ F の生年月日	ユーザ A の生年月日
	年齢	ユーザ F の年齢	ユーザ A の年齢(35 才)
	性別	ユーザ F の性別(男)	ユーザ A の性別(男)
	ユーザの ID	ユーザ F の ID	ユーザ A の ID
	パスワード	ユーザ F のパスワード	ユーザ A のパスワード
従属 ユーザ 情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザの ID		
	パスワード		
利用ポイント情報		レシーバ 51 の利用 ポイント情報	レシーバ 201 の利用 ポイント情報

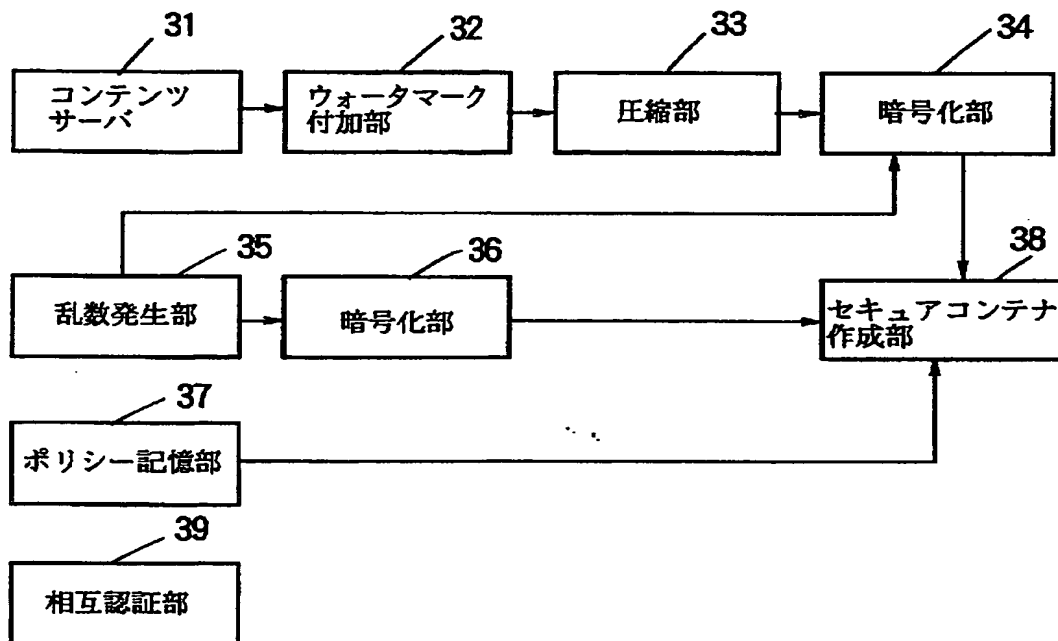
## システム登録情報

【図 1 0】

ユーザ	プロバイダ	利用ポイント
決済 ユーザ	コンテンツプロバイダ 2-1	222 ポイント
	コンテンツプロバイダ 2-2	123 ポイント
	サービスプロバイダ 3-1	345 ポイント
	サービスプロバイダ 3-2	0 ポイント

利用ポイント情報

【図 1 1】



コンテンツプロバイダ 2-1

【図 1 2】

(B)

コンテンツの ID	コンテンツ A の ID
コンテンツプロバイダの ID	コンテンツプロバイダ 2-1 の ID
UCP の ID	ucpB の ID
UCP の有効期限	ucpB の有効期限
利用条件 20	ユーザ条件 20
	機器条件 20
利用内容 21	ID 21
	形式 21
	パラメータ 21
	管理移動許可情報 21
利用内容 22	ID 22
	形式 22
	パラメータ 22
	管理移動許可情報 22

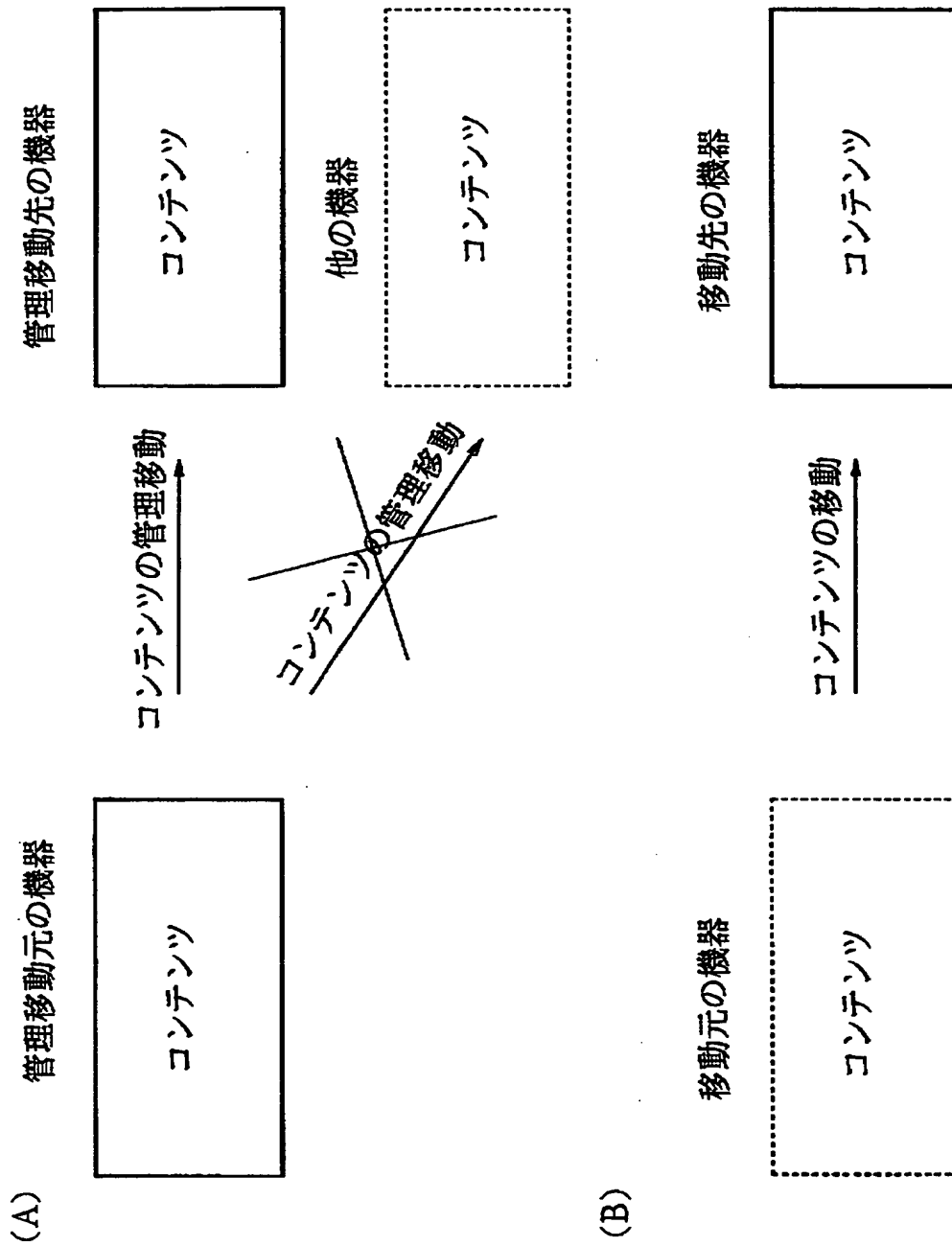
ucpB

(A)

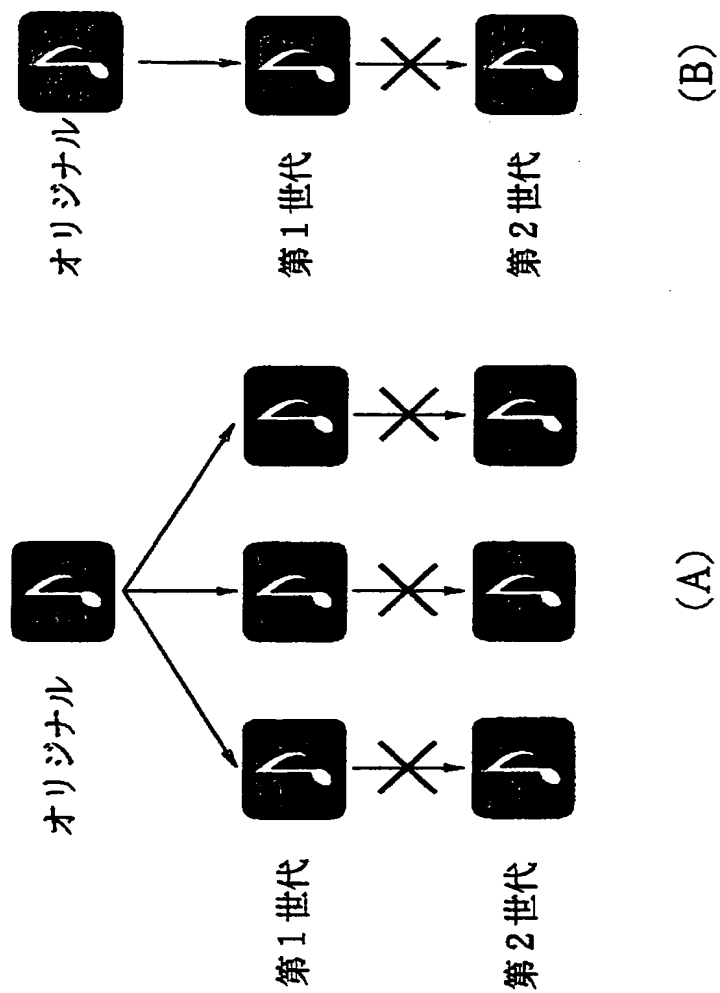
コンテンツの ID	コンテンツ A の ID
コンテンツプロバイダの ID	コンテンツプロバイダ 2-1 の ID
UCP の ID	ucpA の ID
UCP の有効期限	ucpA の有効期限
利用条件 10	ユーザ条件 10
	機器条件 10
利用内容 11	ID 11
	形式 11
	パラメータ 11
	管理移動許可情報 11
利用内容 12	ID 12
	形式 12
	パラメータ 12
	管理移動許可情報 12
利用内容 13	ID 13
	形式 13
	パラメータ 13
	管理移動許可情報 13
利用内容 14	ID 14
	形式 14
	パラメータ 14
	管理移動許可情報 14

ucpA

【図 1 3】



【図 14】



【図 15】

(A)

サービスコード	意 味
0000h	条件なし
0001h 乃至 00FFh	機器に関し条件有り
0100h 乃至 01FFh	性別条件あり
0200h 乃至 02FFh	年令条件あり
0300h 乃至 7FFFh	その他の条件あり
8000h 乃至 FFFFh	利用ポイントに関し条件有り

(B)

コンディションコード	意 味
00h	無条件
01h	=
02h	≠
03h	<(より小さい)
04h	>(より大きい)
05h	≤(以下)
06h	≥(以上)
07h 乃至 FFh	空き



【図 16】

(A)

ユーザ条件 10	サービスコード	バリュースコード	コンディションコード
	80××h	0000C8h	06h
機器条件 10	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

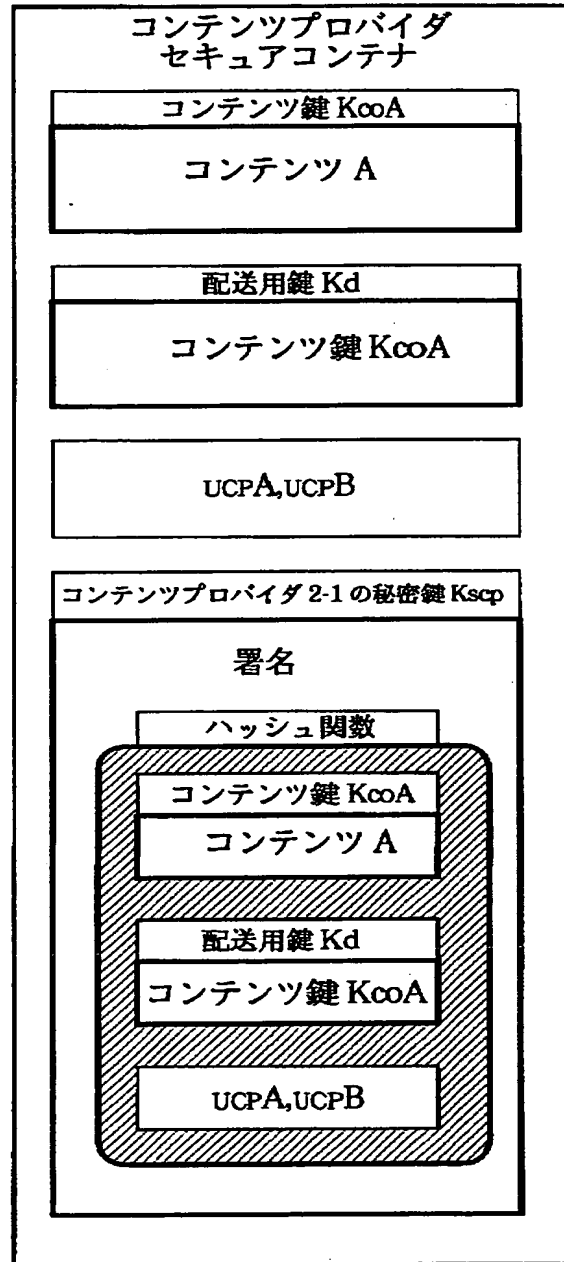
## UCPA の利用条件 10

(B)

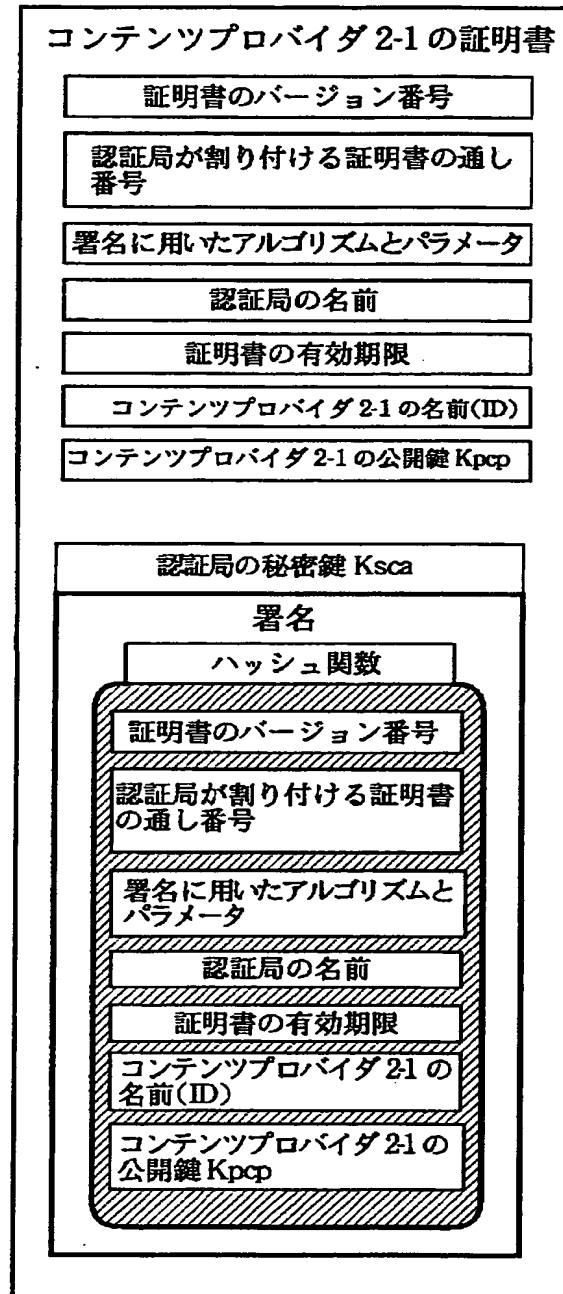
ユーザ条件 20	サービスコード	バリュースコード	コンディションコード
	80××h	0000C8h	03h
機器条件 20	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

## UCPB の利用条件 20

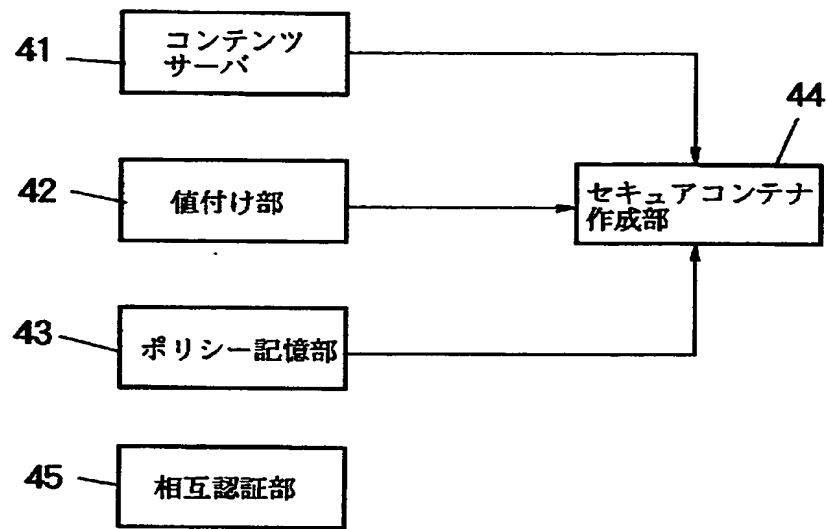
【図 17】



【図 18】



【図 19】



サービスプロバイダ 3-1

【図 2 0】

(B)

コンテンツの ID	コンテンツ A の ID	
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID	
UCP の ID	ucpA の ID	
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID	
PT の ID	PtA-2 の ID	
PT の有効期限	PtA-2 の有効期限	
価格条件 20	ユーザ条件 20	女性
	機器条件 20	条件なし
価格内容 21	1000 円	
価格内容 22	300 円	
価格内容 23	50 円	
価格内容 24	150 円	

PTA-2

(A)

コンテンツの ID	コンテンツ A の ID	
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID	
UCP の ID	ucpA の ID	
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID	
PT の ID	PTA-1 の ID	
PT の有効期限	PTA-1 の有効期限	
価格条件 10	ユーザ条件 10	男性
	機器条件 10	条件なし
価格内容 11	2000 円	
価格内容 12	600 円	
価格内容 13	100 円	
価格内容 14	300 円	

PTA-1

【図 21】

(A)

ユーザ 条件 10	サービスコード	バリューコード	コンディションコード
	01 × × h	000000h	01h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1 の価格条件 10

(B)

ユーザ 条件 20	サービスコード	バリューコード	コンディションコード
	01 × × h	000001h	01h
機器 条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2 の価格条件 20

【図 2 2】

コンテンツの ID	コンテンツ A の ID
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID
UCP の ID	ucpB の ID
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID
PT の ID	ptB-2 の ID
PT の有効期限	ptB-2 の有効期限
価格条件 40	ユーザ条件 40
	機器条件 40
価格内容 41	
価格内容 42	

ptB-2  
(B)

コンテンツの ID	コンテンツ A の ID
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID
UCP の ID	ucpB の ID
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID
PT の ID	ptB-1 の ID
PT の有効期限	ptB-1 の有効期限
価格条件 30	ユーザ条件 30
	機器条件 30
価格内容 31	
価格内容 32	

ptB-1  
(A)

【図 23】

(A)

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00xxh	000064h	03h

PTB-1 の価格条件 30

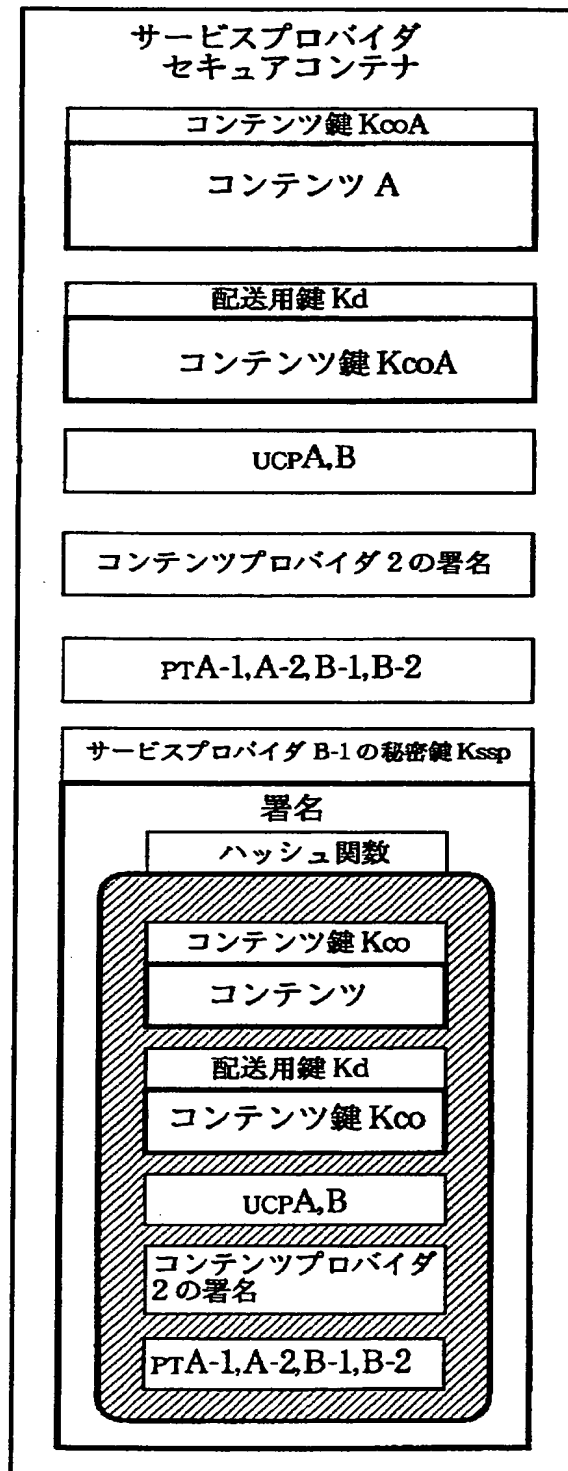
(B)

ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00xxh	000064h	06h

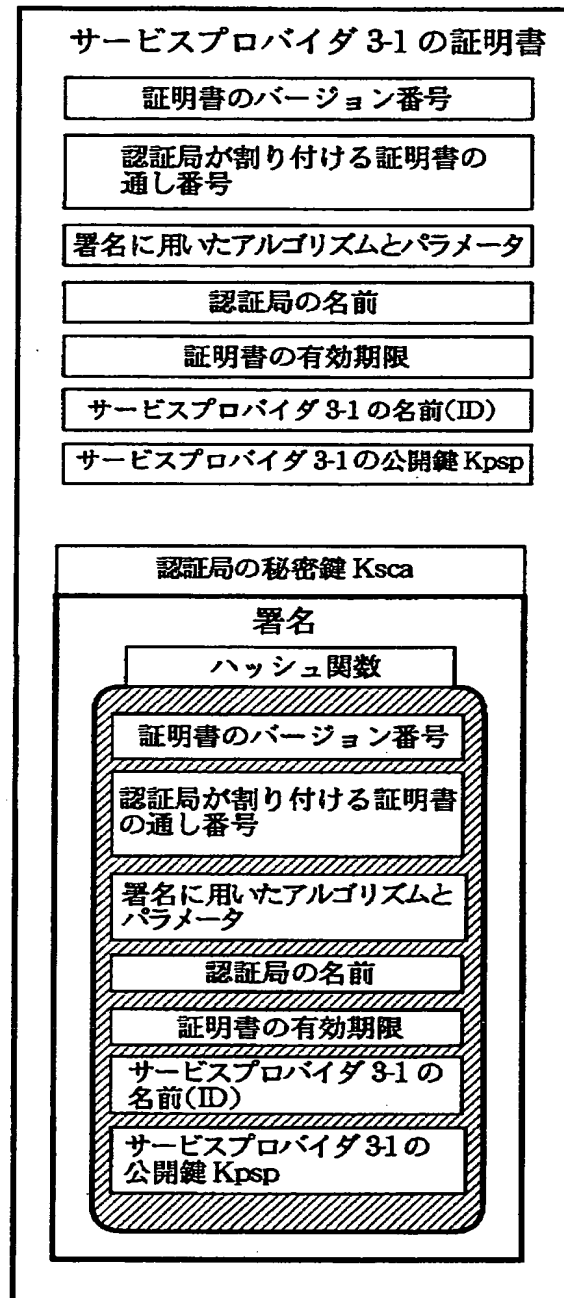
PTB-2 の価格条件 40



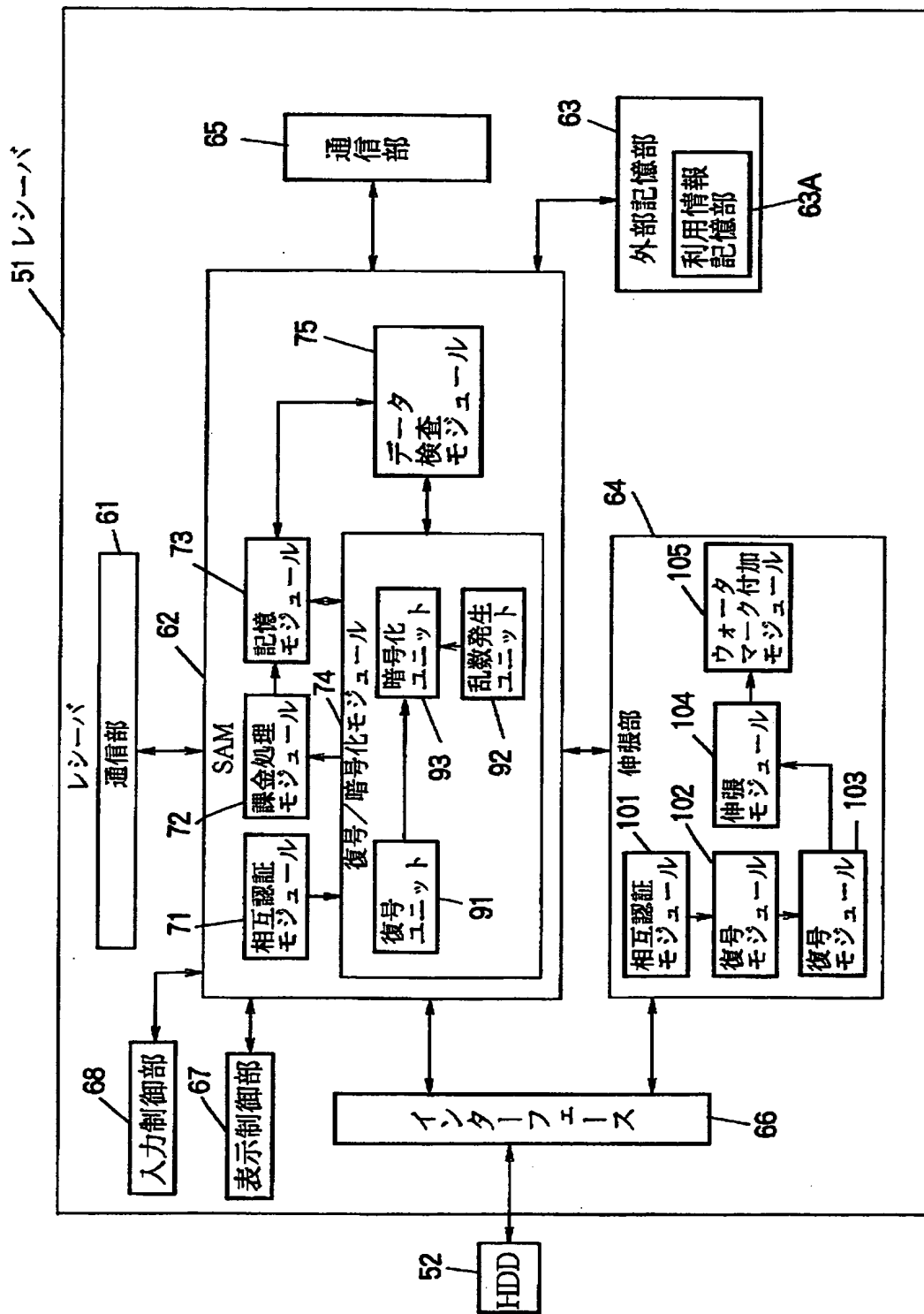
【図 24】



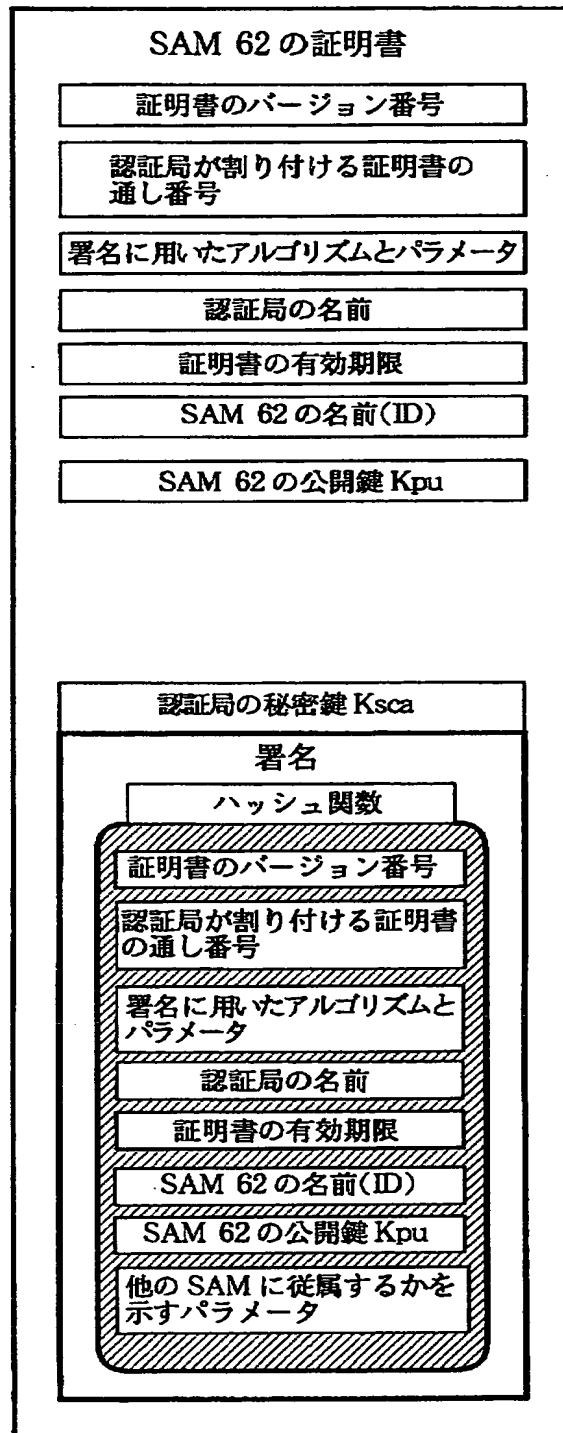
【図 25】



【図 2 6】



【図 27】

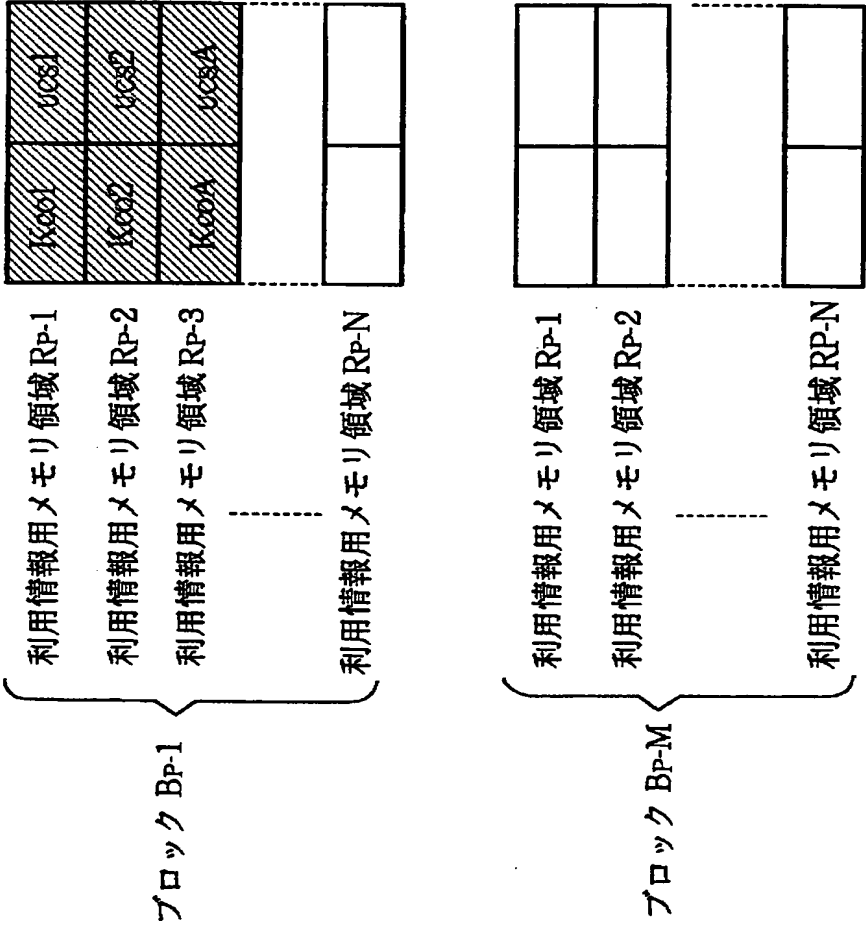


【図 2 8】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2-1 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3-1 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 11 の ID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動 状態情報	管理移動元 : SAM62 の ID、 管理移動先 : SAM62 の ID
利用履歴		× × ×

ucsA

【図 2 9】



利用情報記憶部 63A

【図 30】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2-1 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3-1 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 11 の ID
	形式	買い取り再生
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
課金履歴		×××

課金情報 A

【図 3 1】

SAM62 の公開鍵 Kpu	
SAM62 の秘密鍵 Ksu	
EMD サービスセンタ 1 の公開鍵 Kpesc	
認証局の公開鍵 Kpca	
保存用鍵 Ksave	
3 月分の配送用鍵 Kd	
.....	
SAM62 の証明書	
基準情報 51	
課金情報	
.....	
検査値 Hp-1	検査値 Hp-2 .....
.....	検査値 Hp-M



【図 3 2】

SAM の ID		SAM62 の ID
機器番号		レシーバ 51 の機器番号 (100 番)
決済 ID		ユーザ F の決済 ID
課金の上限額		正式登録時の課金の 上限額
決済 ユーザ 情報	氏名	ユーザ F の氏名
	住所	ユーザ F の住所
	電話番号	ユーザ F の電話番号
	決済機関情報	ユーザ F の決済機関情報
	生年月日	ユーザ F の生年月日
	年齢	ユーザ F の年齢(21 才)
	性別	ユーザ F の性別(男)
	ユーザの ID	ユーザ F の ID
	パスワード	ユーザ F のパスワード
従属 ユーザ 情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザの ID	
	パスワード	
⋮		
利用ポイント情報		レシーバ 51 の利用 ポイント情報

基準情報 51

【図 33】

ユーザ	プロバイダ	利用ポイント
決済 ユーザ	コンテンツプロバイダ 2-1	222 ポイント
	コンテンツプロバイダ 2-2	123 ポイント
	サービスプロバイダ 3-1	345 ポイント
	サービスプロバイダ 3-2	0 ポイント

基準情報 51 の利用ポイント情報

【図 3 4】

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテナ供給機器	状態フラグ	登録条件署名	登録リス ト署名	
レシーバ 51の登録 条件 SAM62の ID	ユーザ F の ID	可	可	SAM62 の ID	なし	制限 なし	××××	××××	
レシーバ 201の 登録リスト SAM212の ID	ユーザ A の ID	可	可	SAM212 の ID	なし	制限 なし	××××	××××	

対象 SAM ID

有効期限

バージョン番号

接続されている機器数

SAM62 の ID

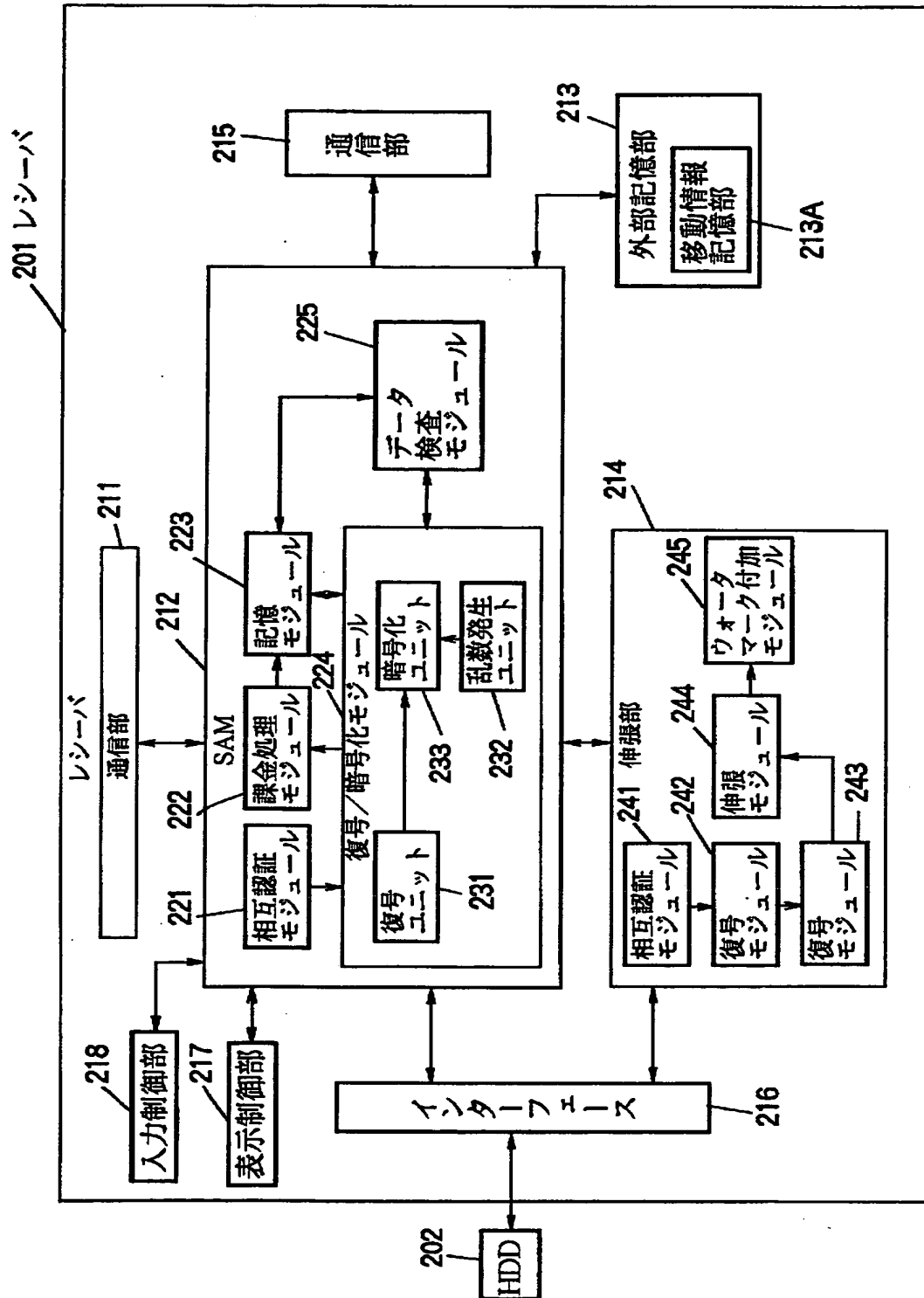
××××

××××

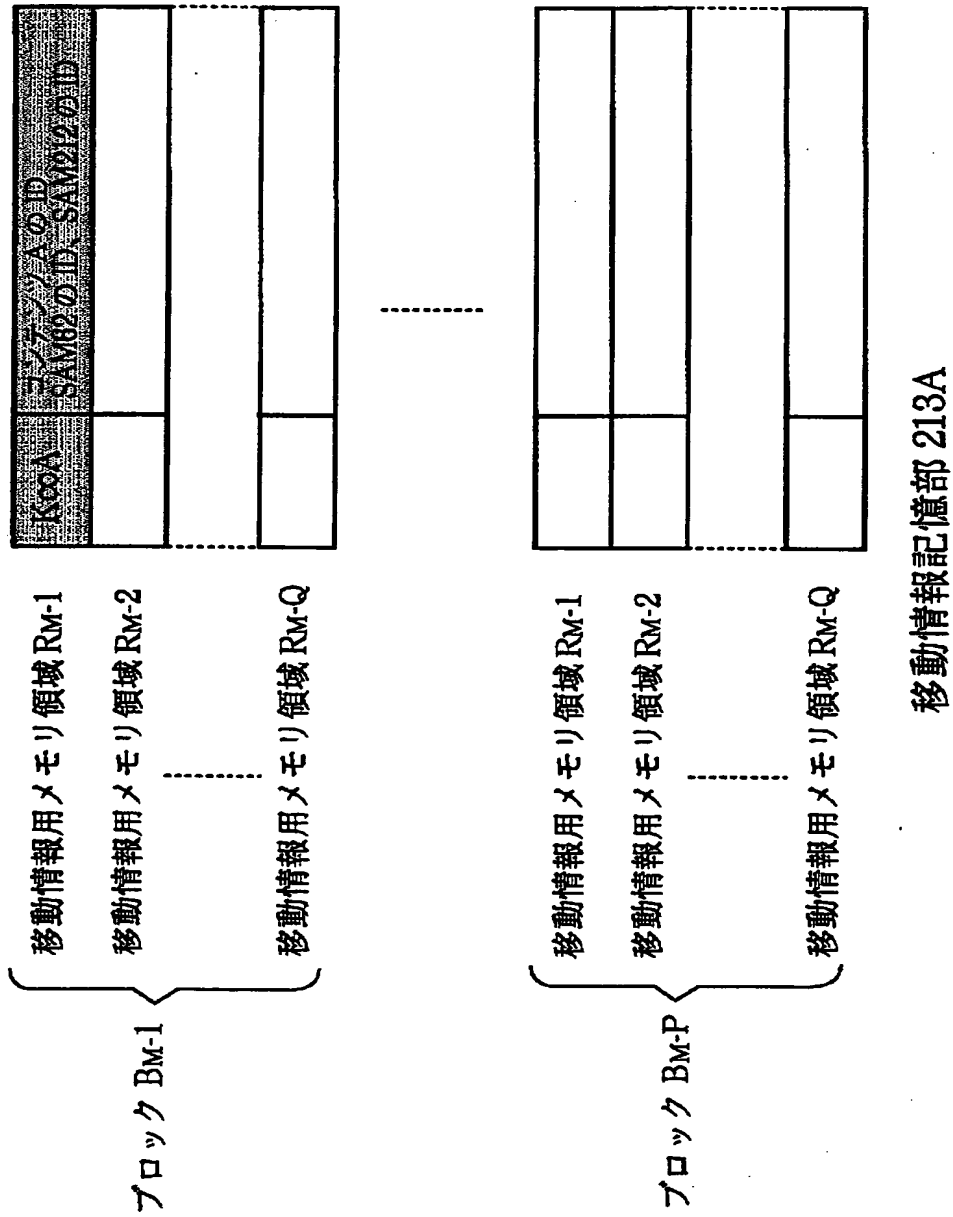
2

対象 SAM 情報部

【図 35】



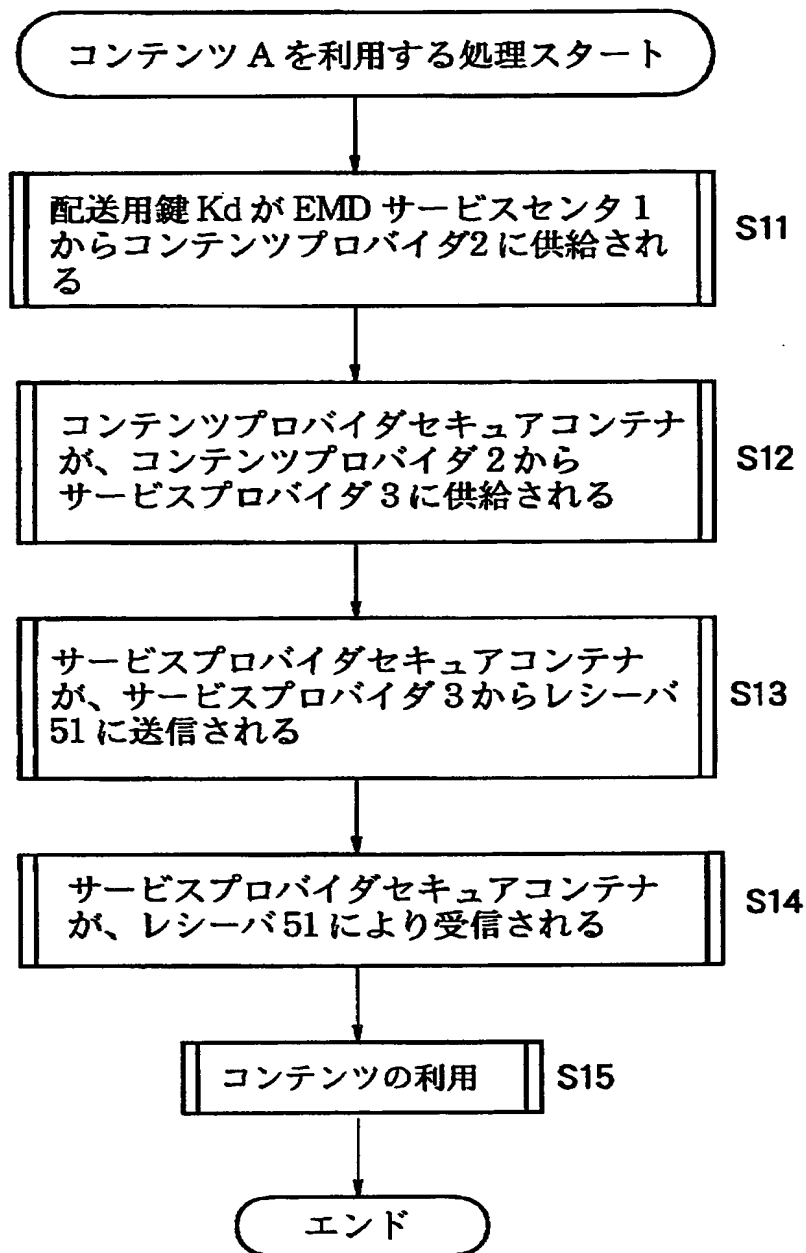
【図 3 6】



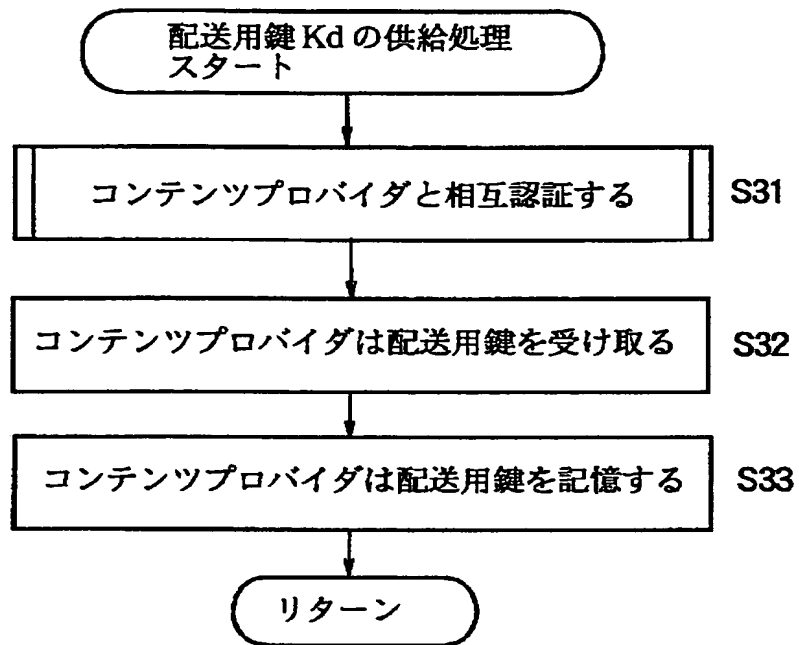
【図 3 7】

SAM212 の公開鍵 Kpu	
SAM212 の秘密鍵 Ksu	
EMD サービスセンタ 1 の公開鍵 kpesc	
認証局の公開鍵 Kpca	
保存用鍵 Ksave	
3 月分の配送用鍵 Kd	
⋮	
SAM212 の証明書	
基準情報 201	
⋮	
検査値 Hm-1	検査値 Hm-2
⋮	
検査値 Hm-P	

【図 38】

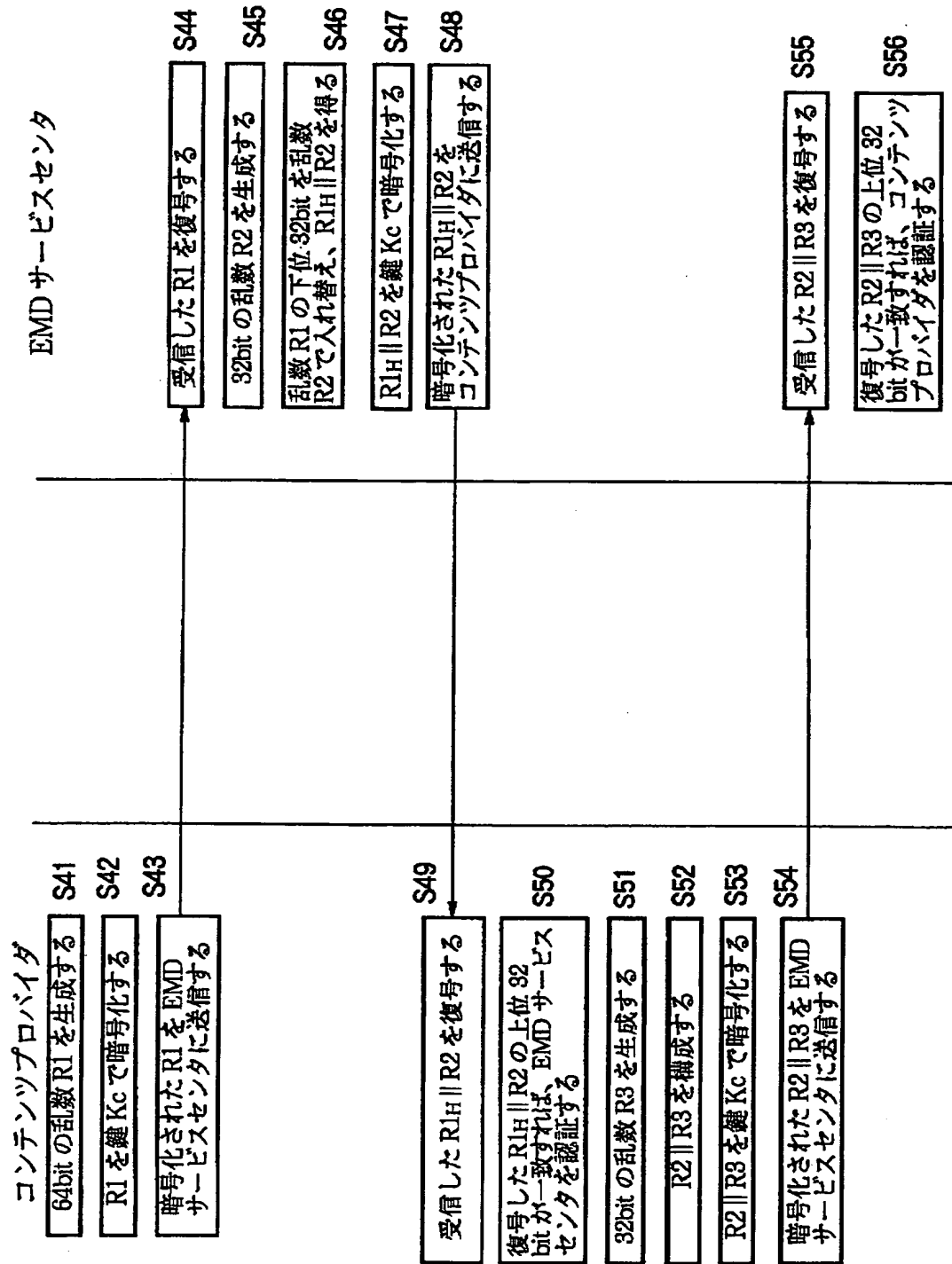


【図 39】

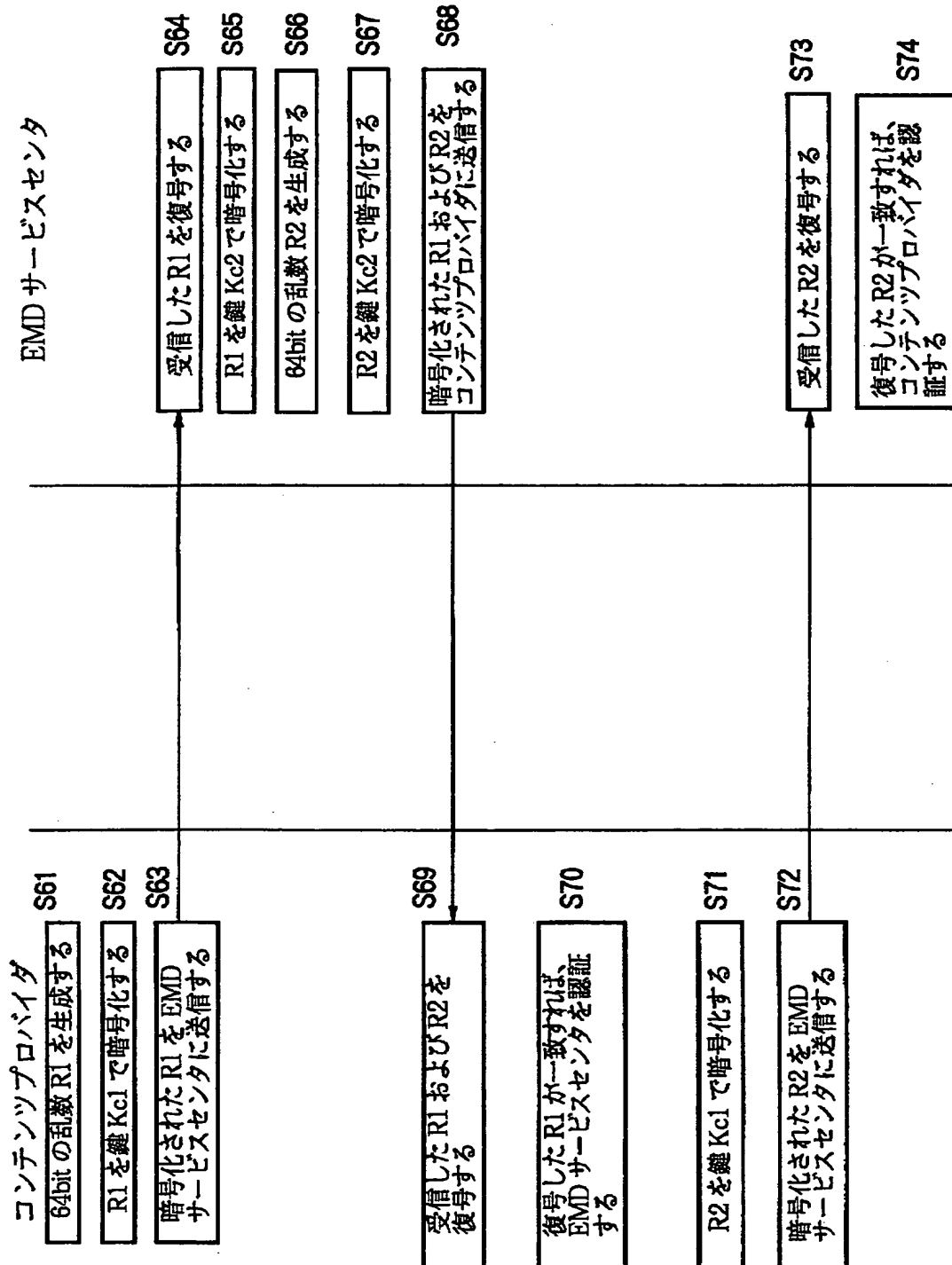




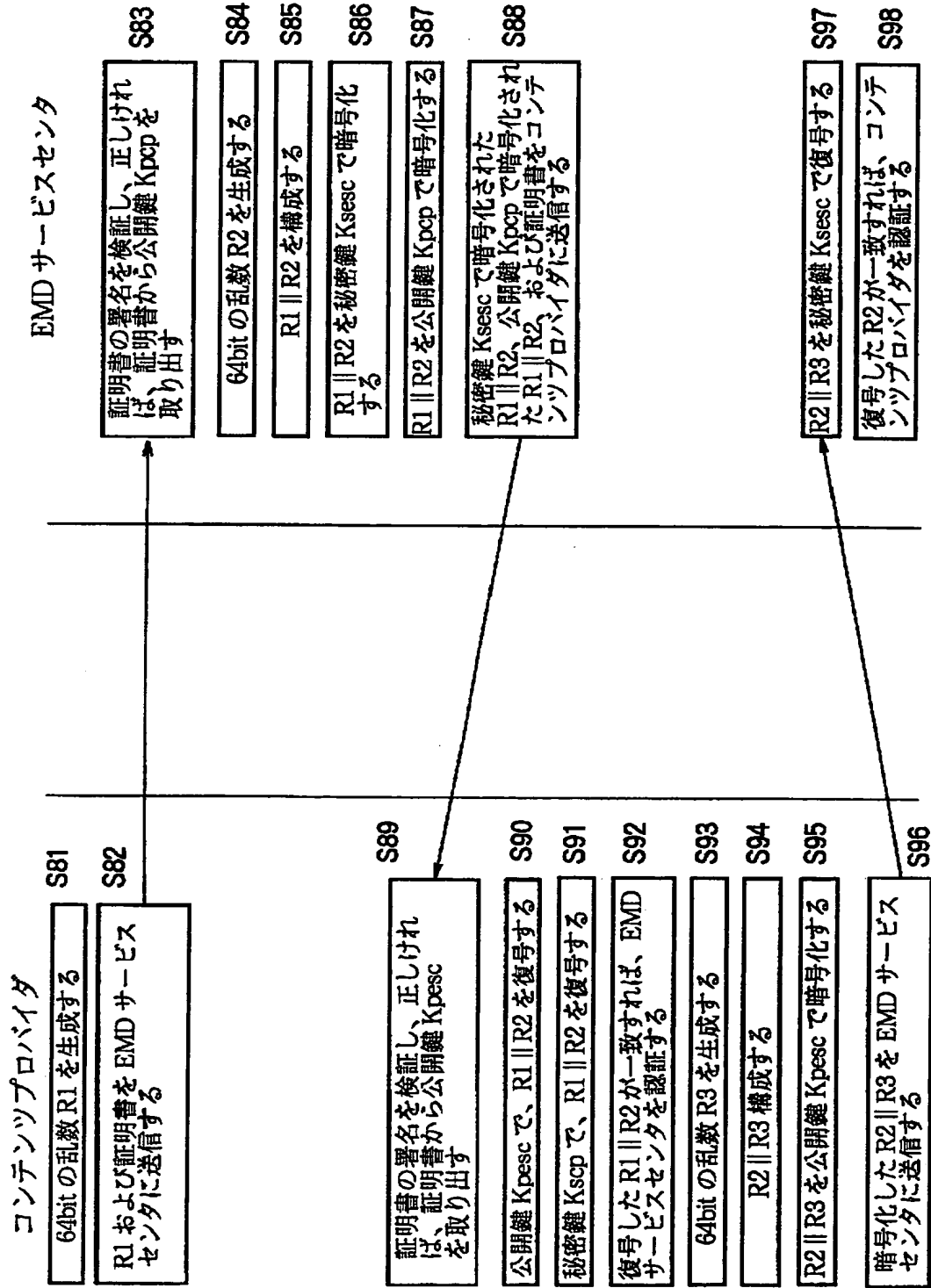
【図 4 0】



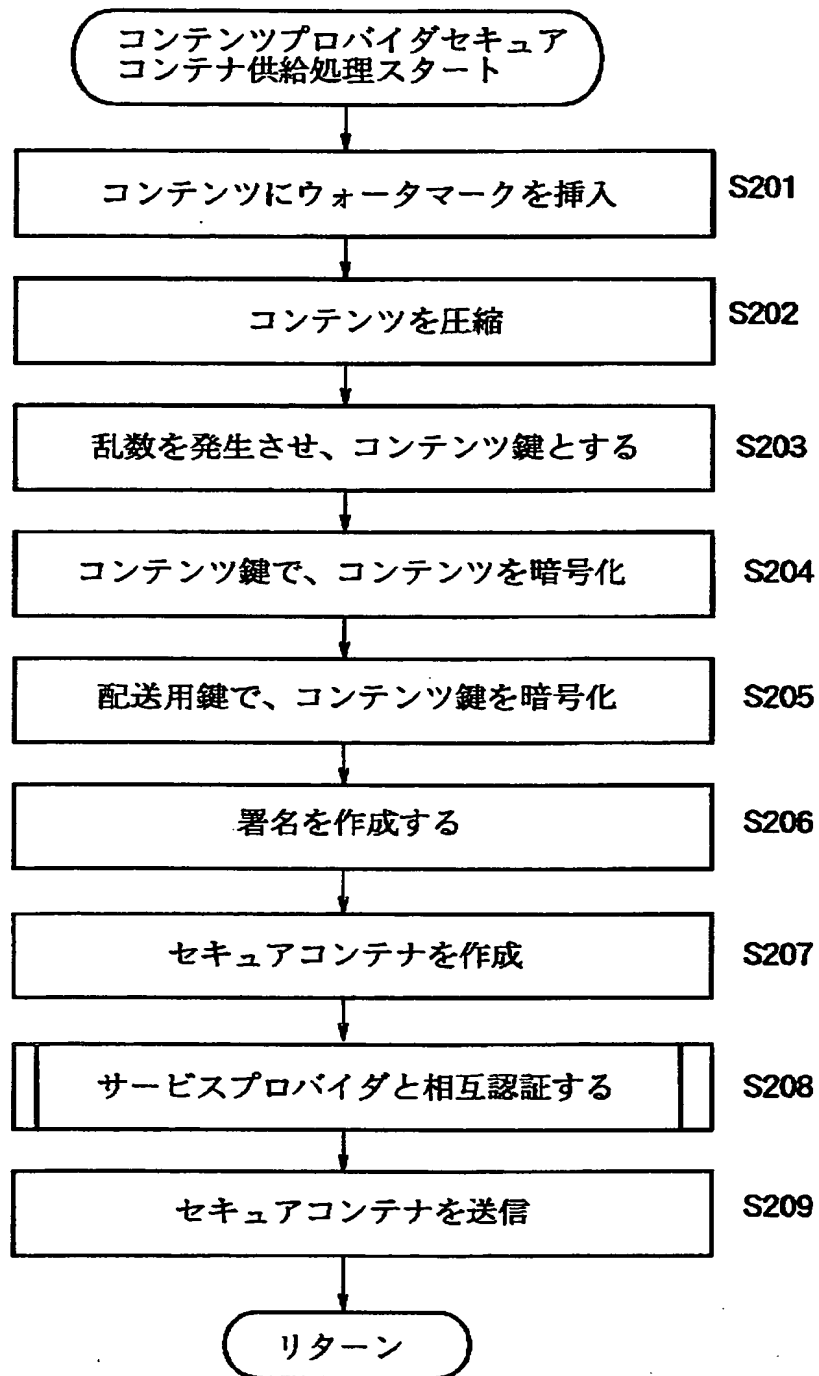
【 図 4 1 】



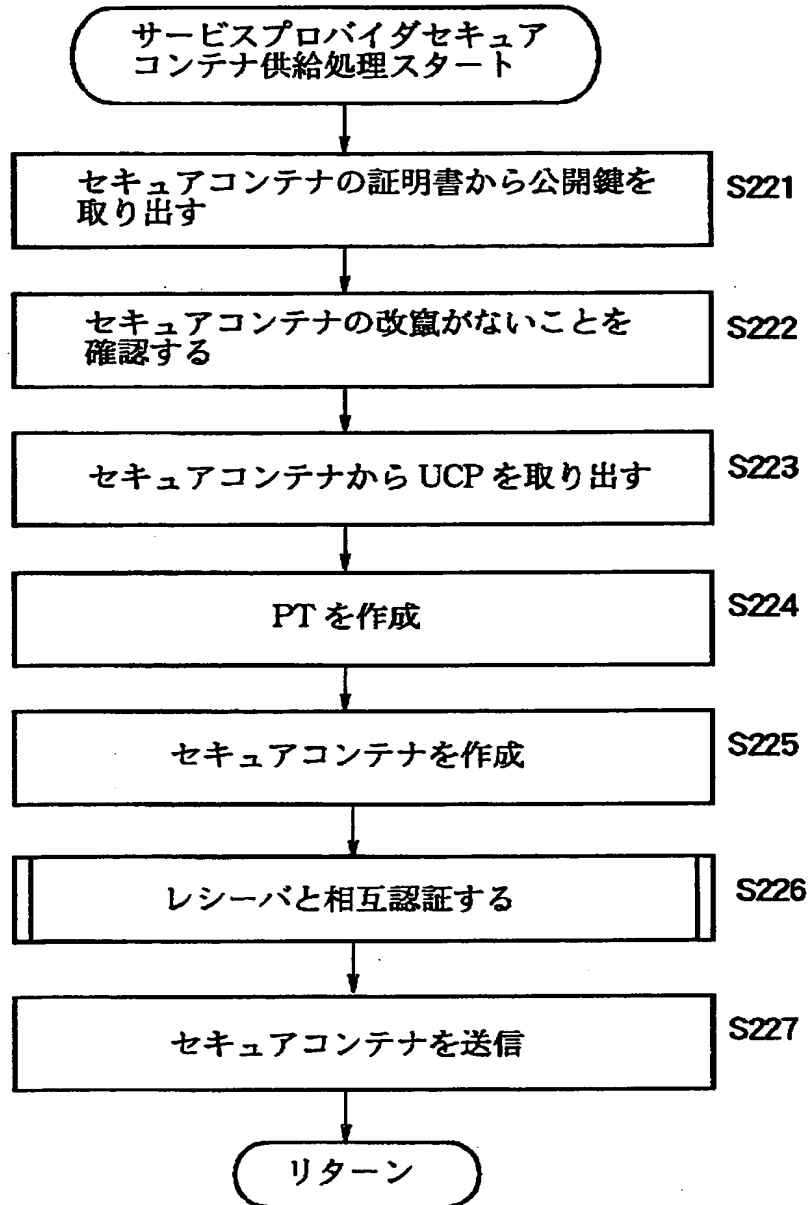
【図 4 2】



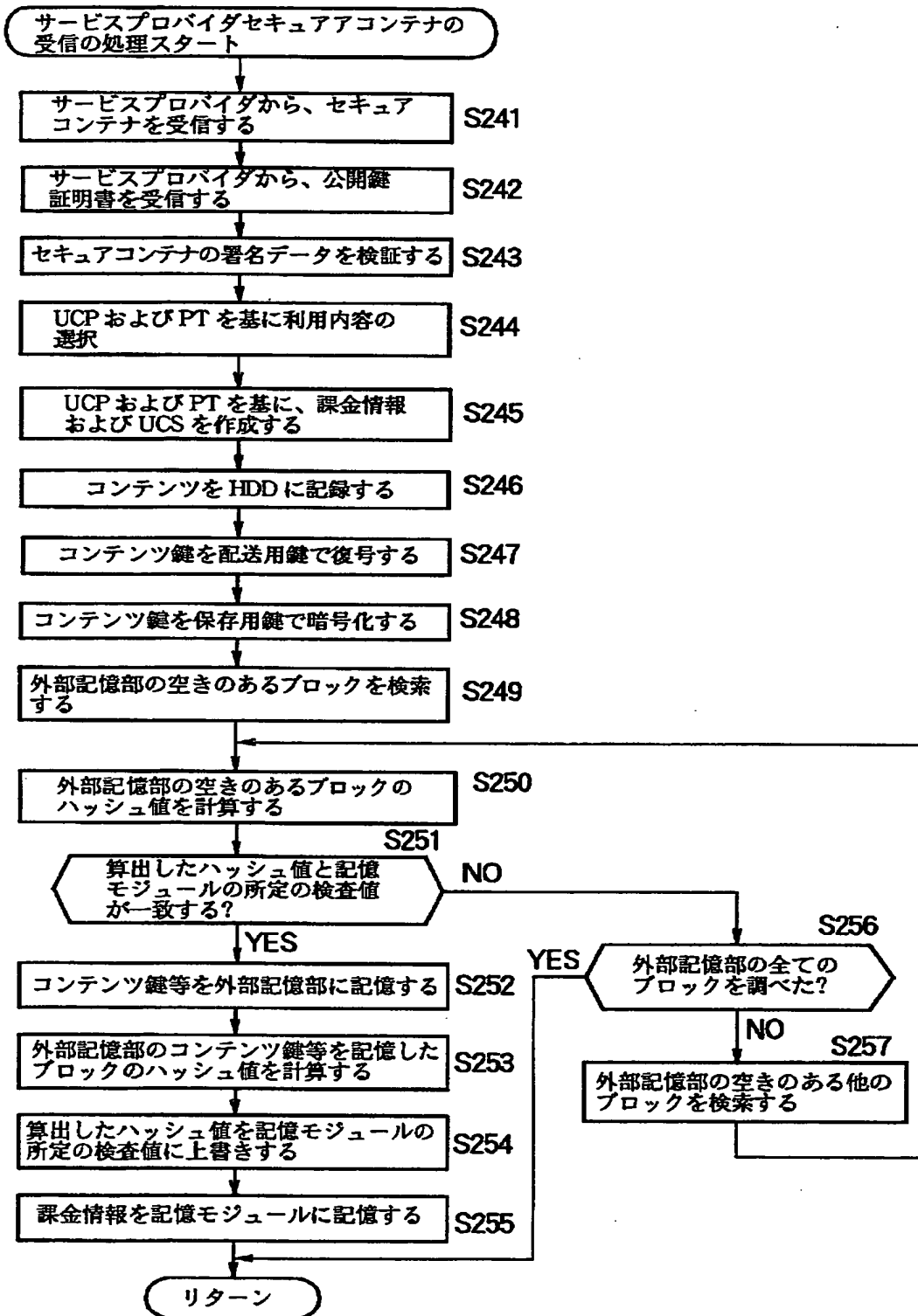
【図 4 3】



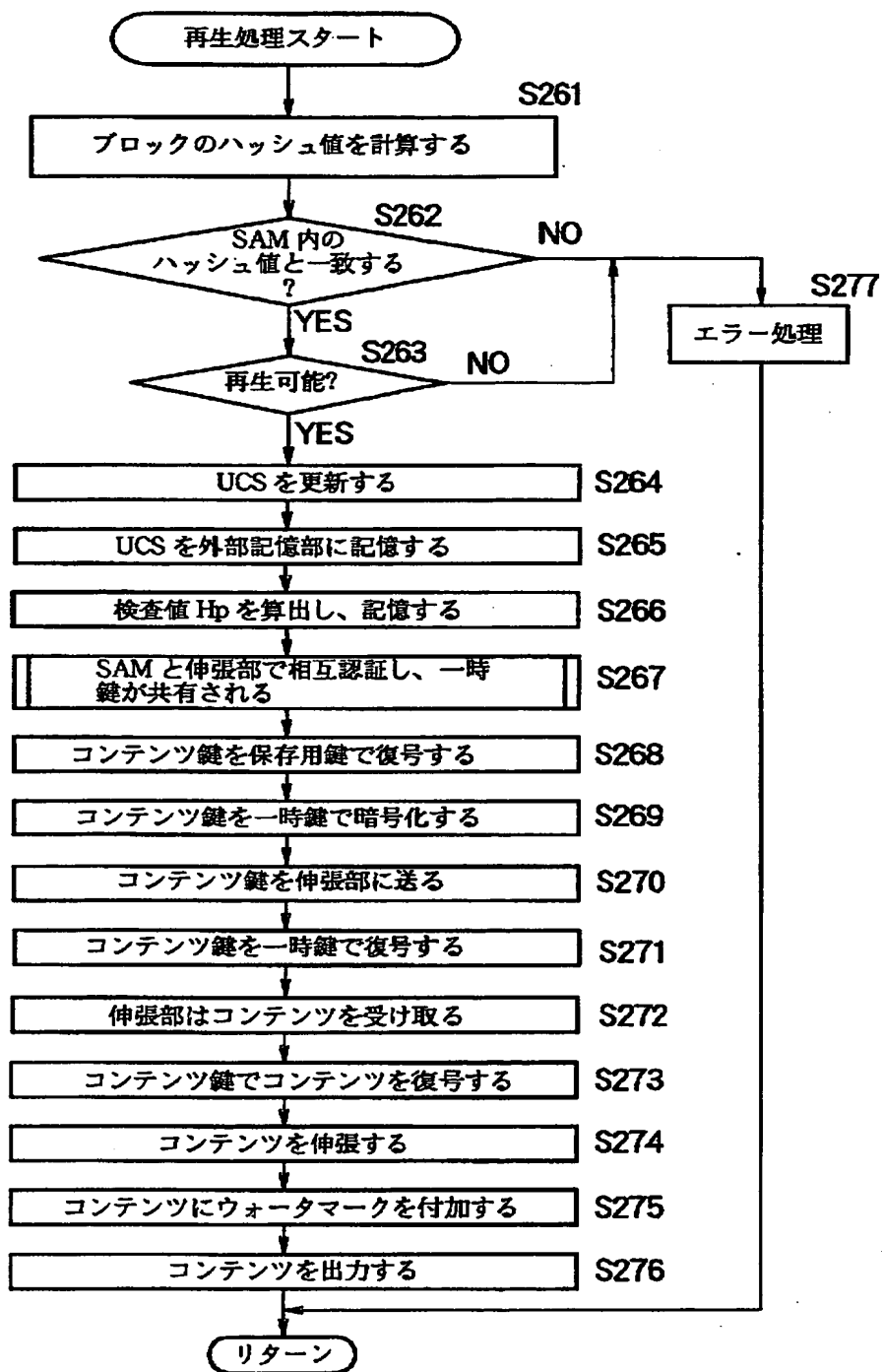
【図 4 4】



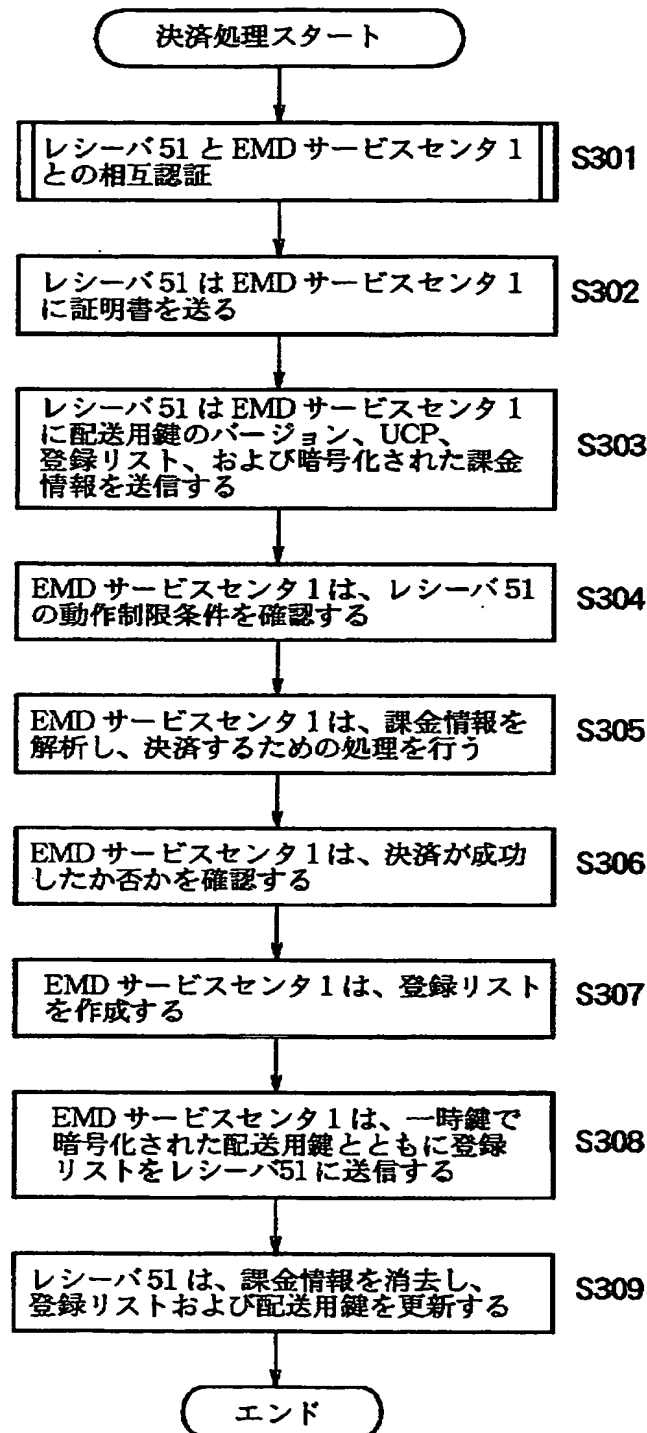
【図 4 5】



【図 4 6】

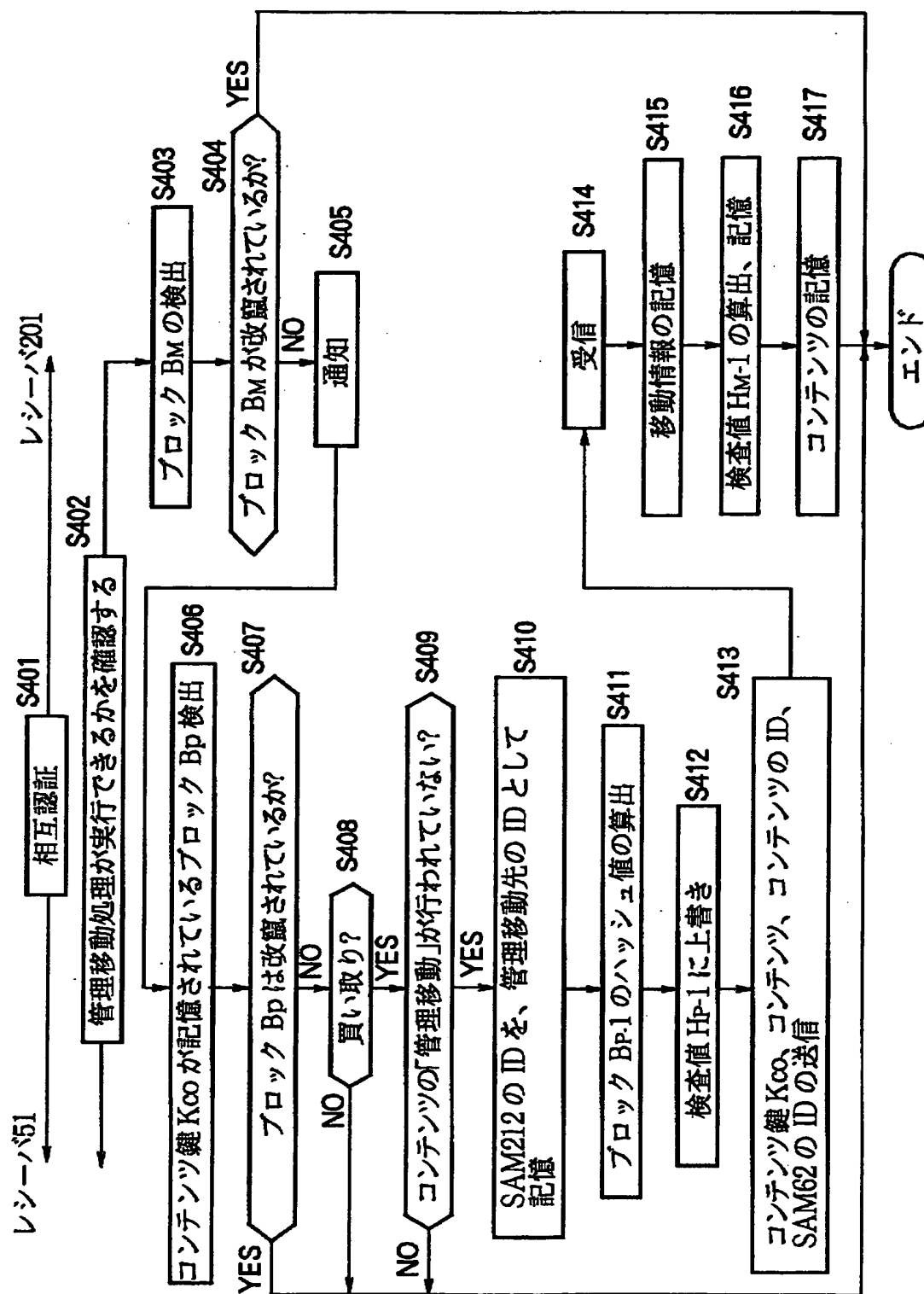


【図 4 7】

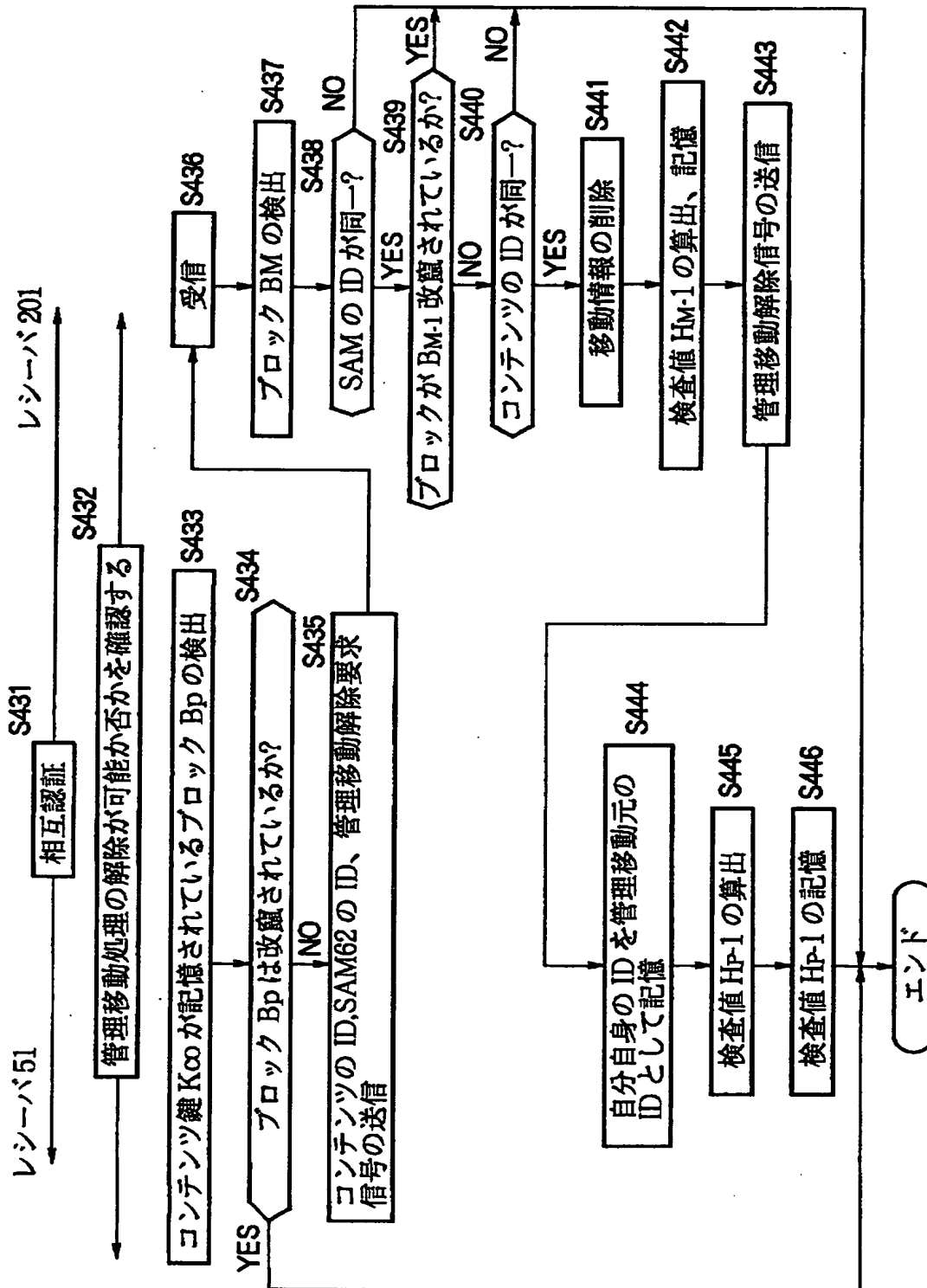




【图 4 8】



【図 4 9】



【書類名】 要約書

【要約】

【課題】 コンテンツの移動元の機器が、コンテンツを保持しつつ、コンテンツを移動させることができるようにする。

【解決手段】 管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。つまり、移動元の機器にコンテンツが保持されず、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。コンテンツの管理移動が行われている間、管理移動元の機器は、他の機器にコンテンツを管理移動することができない。管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。つまり、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世代の複製とも異なる。管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、1回だけの複製とも異なる。

【選択図】 図13

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社